Advanced Endpoint Protection:
Fileless Threats Protection test

The test is commissioned by Kaspersky and performed by AV-TEST GmbH. Date of the report: September 27th 2019

Executive Summary

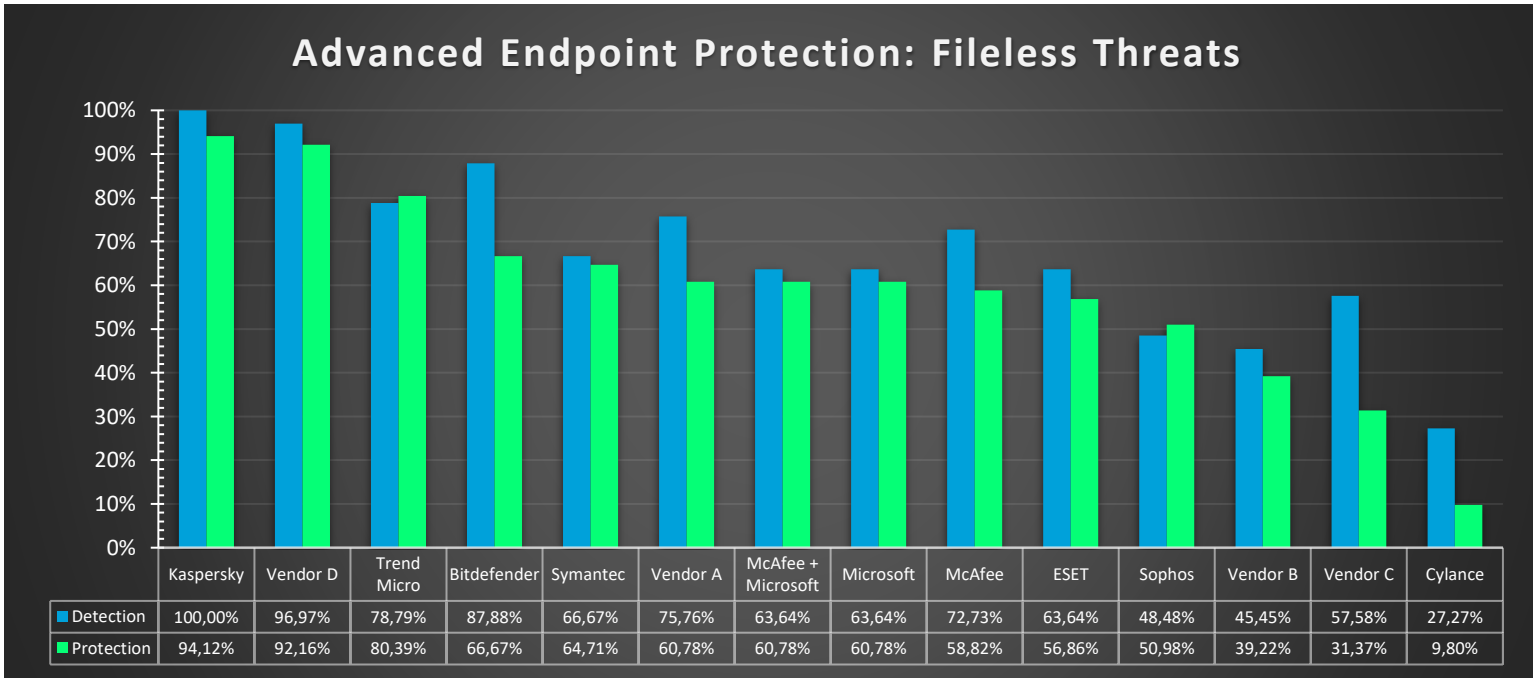
In May 2019 AV-TEST performed a test of Fileless Threats Protection by different endpoint security products. In total 33 different fileless attacks, divided into four categories have been used to test 14 products. The test aimed to reveal ability of the products to detect fileless threats (so to measure Detection Rate) and ability to Protect and Remediate all malicious actions by fileless threats (Protection Rate).

The test cases were created in-house by using well known frameworks and publicly well documented attacking techniques with intention to cover as much fileless techniques as possible. The used techniques included malware execution from WMI storage and via the Task Scheduler as well as Powershell and other scripts. Additionally, a false positive test was carried out. All tests were performed on Windows 10, with Microsoft Office installed.

During the test, the products were expected to detect the different attacks and prevent or remediate the malicious actions. The best Detection results were achieved by Kaspersky with a 100% detection rate while the average detection of all products was at 67.75%. The best Protection Rate of 94.12% was achieved again by Kaspersky while the average protection level of all products turned out 59.10%. 11 out of 14 products finished with zero False Positives in both Detection and Protection parts. For more detailed information refer to section 'Test Results' of the report.

The test results show that nowadays not all vendors are able to detect fileless threats and protect endpoint systems. Keeping in mind the proliferation of fileless techniques utilization from only targeted attacks to attacks onto regular users, we consider important for security vendors to improve their technologies significantly, no matter what they promise by their marketing.

No product results were excluded from the report to keep the security picture complete.



	Kaspersky	Vendor D	Trend Micro	Bitdefender	Symantec	Vendor A	McAfee + Microsoft	Microsoft	McAfee	ESET	Sophos	Vendor B	Vendor C	Cylance
Detection	100,00%	96,97%	78,79%	87,88%	66,67%	75,76%	63,64%	63,64%	72,73%	63,64%	48,48%	45,45%	57,58%	27,27%
Protection	94,12%	92,16%	80,39%	66,67%	64,71%	60,78%	60,78%	60,78%	58,82%	56,86%	50,98%	39,22%	31,37%	9,80%

Introduction

Fileless attacks is a growing dangerous trend in current cyber-threat landscape. Such techniques were mostly used for targeted attacks (APT) in past years, but now they are seen more often in commodity attacks as well. Security experts already spotted utilization of fileless techniques in different types of wide-spread malware, including new families of trojans, ransomware, illegal crypto-miners, and even adware. One of the striking examples is PowerGhost, a fileless multi-tool for both crypto-mining and DDoS attacks, that infected many corporate computers. Fileless malware popularity is obviously caused by their ability to evade anti-malware technologies.

What is special about these attacks is the lack of file-based components. Threat actors can deliver fileless payloads to a victim's machine via different methods such as drive-by attacks, malicious documents with macros or vulnerability exploitation. However, instead of downloading malicious files to the disk and executing them, fileless malware hides the malicious code in memory or in legitimate Windows system storages (WMI objects, task scheduler objects, etc) and executes it from there abusing legitimate applications and utilities. In general, use of system-based tools for fileless threats allows an attacker to achieve effective persistence on victim's host.

Fileless attack detection and remediation became a serious challenge for many security solutions since it requires the implementation of a whole set of new, more profound technologies. To discover fileless threats, a security solution has to inspect different kinds of OS storages (Windows Registry content, WMI objects, task scheduler objects, etc) and analyze execution patterns of processes in the system in real time. In case of true negative detection, a security solution must be able to clear deeply-hidden fileless infection out of the system, while preventing false positives over execution of legitimate admin actions. Such protective measures against fileless malware could not be provided neither by simple signature-based techniques nor by advanced machine learning-based file inspection methods - no matter how these methods are praised in the market.

We run this test to discover how marketing promises of efficient fileless threat protection, claims about unbelievable advantages of some protective tools, and different ad slogans correlate with reality. This test is aimed to show what fileless malware can do and which security products are capable of detecting, blocking and remediating fileless attacks - irrespective of what is claimed by security vendors themselves.

Contents

Test Methodology

The test has been carried out according to the information below.

The report contains all results of all products initially requested into the test, none of them were excluded from the report independently on reached results. There was no feedback process for this test.

During Detection part of the test, we recorded for each security solution if it was able to flag a warning against executed actions. In Protection part, we recorded if a security solution was able to protect and\or remediate every malicious action of the attack.

Tested Products

All tested products are listed in the tab below. The products of Carbon Black, CrowdStrike, Palo Alto and SentinelOne are listed as "Vendor A" to "Vendor D" (in random order) due to restrictions of their results publication. The products were tested in default configuration.

Product Name	Version
Bitdefender Business Security	6.6.9.134
Cylance Protect	2.0.1530.5
ESET Endpoint Security	7.0.2091.0
Kaspersky Endpoint Security for Business	11.0.1.90
McAfee Endpoint Security	5.5.0.447
McAfee Mvision + Microsoft Defender	MVISION: 5.6.0.878, Defender: 4.12.17007.18022
Microsoft Defender Antivirus	4.12.17007.18022
Sophos Central Endpoint	10.8.3
Symantec Endpoint Protection	14.2.770.0000
Trend Micro Endpoint Apex	13.95.1165
Vendors A to D	n/a

Test Environment

An attacking host based on KALI LINUX was used to prepare and carry out the attacks. The attacked host were running Microsoft Windows 10 RS3 with Microsoft Office 2013 and the tested product installed. Extra attacked host without tested product was used to verify the attack execution concept. The attacked hosts were prepared to have a secret.docx file in the folder c:\users\vtc\Documents\secret.docx. Connections to the FTP and HTTP server on the KALI Linux machine were checked before running the tests.

The HTTP and FTP servers were prepared as follows:

HTTP Server on Kali:

- *from a terminal*
- *apache2ctl start|stop|restart|graceful|*

FTP Server on Kali:

- *apt-get install python-pyftpdlib*
- *run "python -m pyftpdlib -p 21 -w" from the ftp dir*

All machines had access to the Internet at all times and antimalware bases were updated.

Test cases

The different attacks used in the test could divided into the following four categories.

Test category 1: Malware execution from WMI storage

Test cases of this category use well-known persistence technique via WMI subscription mechanism in Microsoft Windows operating system. Two main infection vectors were tested:

- WMI subscription was installed after PowerShell command was executed (in an in-the-wild scenario it could be done after exploitation process or malicious office macros execution)
- WMI subscription was installed after malicious LNK file was executed.

In all the test cases, a first stage PowerShell script was executed using WMI subscription after victim "log on" action. First stage PowerShell script aims at downloading second stage PowerShell script from remote web server. Similar techniques are widely used by APTs, and Adware.

In total four test cases were prepared and tested.

Test category 2: Malware execution by Task Scheduler

In this category, Task Scheduler (legitimate component of Microsoft Windows) is used to perform persistence and execution on victim's host. Malicious Task Scheduler task is installed with the help of execution PowerShell command or with the help of Microsoft Office exploit CVE-2017-0199. In In-The-Wild (ITW) attacks, it is usually performed after vulnerability exploitation, malicious office macros or just malicious executable file execution. Main functionality of installed Task Scheduler task is to download and execute second stage PowerShell script from remote host. In this scenario, different ways of second stage execution were used, including:

- Execution of meterpreter payload
- Execution of meterpreter payload with the help of ReflectivePEInjection technique
- Execution of malicious payload which is stored in legitimate resource e.g. pastebin

In total ten test cases were prepared and tested.

Test category 3: Running Powershell script after execution of Exploit/Macros

In this category, different techniques and methods are used for fileless persistence in victim's machine. In all cases as a final payload meterpreter is used. Examples of attacks:

- Malicious office document with macros which is using PowerShell and Invoke-ReflectivePEInjection for meterpreter execution. All malicious content is downloaded from attackers remote host.
- Malicious office document that is using vulnerability for CVE-2017-0199. After successful exploitation, PowerShell and Invoke-ReflectivePEInjection are used for meterpreter execution.

In total two test cases were prepared and tested.

Test category 4: Other approaches

This category of test cases contains mix of different In-The-Wild (ITW) fileless techniques including:

- Usage of file associations for malware execution
- Usage of SettingContent-MS File Execution Vulnerability
- Remote sct files execution

Additionally legitimate utilities are used in these scenarios for remote commands execution. The utilities are used in APT attacks for lateral movement. In addition, such techniques are used by ITW malware for spreading in victim's network. The following technique is used:

- PsExec legitimate utility for launching malicious xsl file on victim host (https://github.com/kmkz/Sources/blob/master/wmic-poc.xsl).

In total seventeen test cases were prepared and tested.

False Positive Test

In this section, we included several test cases, which are used by administrators in legitimate cases but threat actors could use similar techniques to infect machine in network. Examples of test cases:

- Usage of PsExec to retrieve information about remote hist
- Usage of WMIC to collect information about running processes on remote host
- Usage of WMI subscription to log activity of running service in host

In total three test cases were prepared and tested.

Scoring

The products were expected to detect the attack and prevent or remediate the malicious actions.

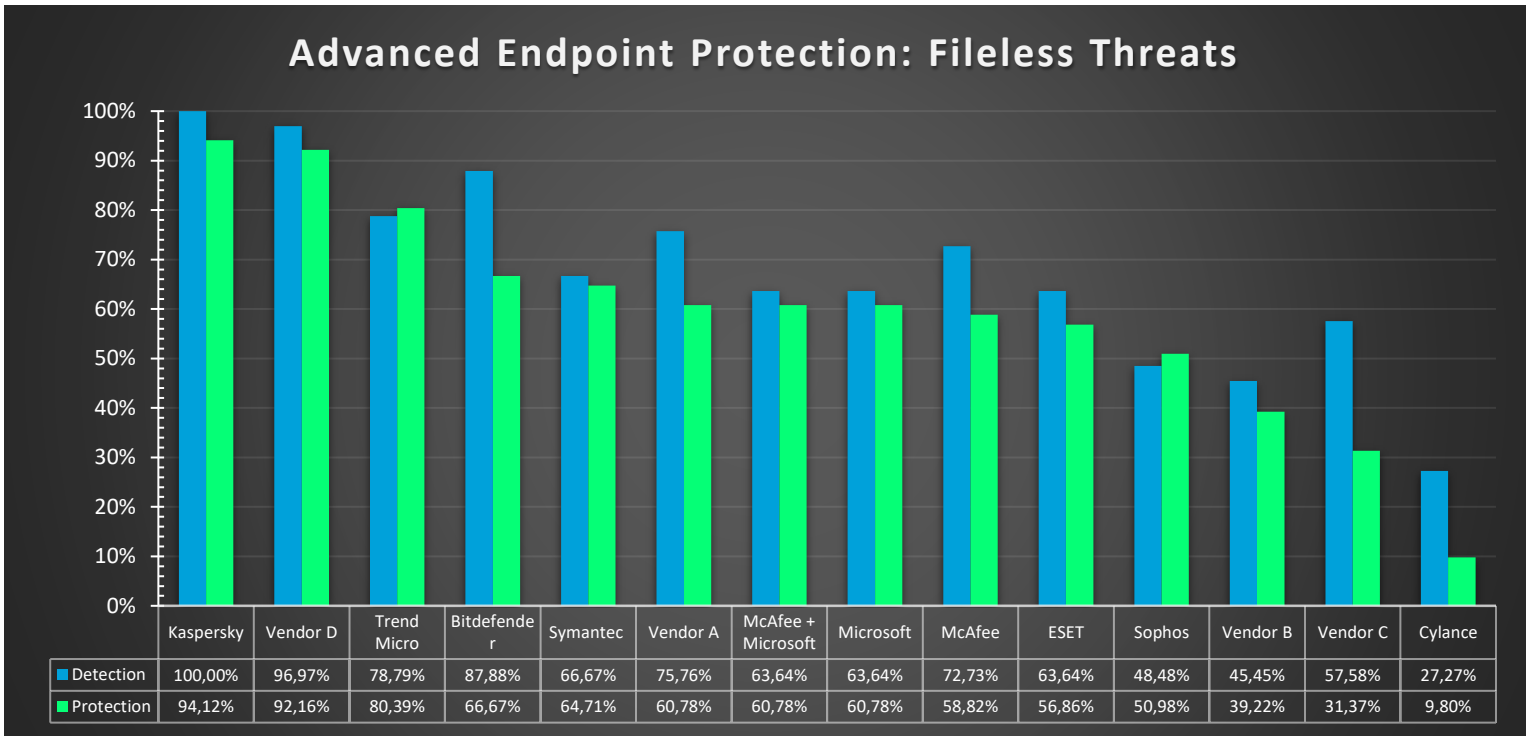
In Detection part of the test, any kind of detection, for example, static or dynamic detection, by Firewall, etc., was considered. Since there were 33 different test cases a maximum of 33 points could be scored here.

In Protection part of the test, all different malicious actions of each test scenario were scrutinized for Prevention or Remediation by product under the test. If the product successfully prevented or remediated an action, then one point was given for each. In total 51 actions were carried out, which this is also the maximum score possible.

The False Positive test consisted of three different fileless based test cases, which should not be detected, furthermore in one case a file was created on disk, which shall not be blocked, by any of the products. For each wrong detection or block one false positive detection was counted.

Test Results: Detection and Protection

The overall Detection Rate and Protection Rate results are depicted in the following graphs: in percentages on Figure 1 and in absolute amount of earned points - on Figure 2. Product results on the graphs are sorted by value of Protection Rate.



	Kaspersky	Vendor D	Trend Micro	Bitdefender	Symantec	Vendor A	McAfee + Microsoft	Microsoft	McAfee	ESET	Sophos	Vendor B	Vendor C	Cylance
Detection	100,00%	96,97%	78,79%	87,88%	66,67%	75,76%	63,64%	63,64%	72,73%	63,64%	48,48%	45,45%	57,58%	27,27%
Protection	94,12%	92,16%	80,39%	66,67%	64,71%	60,78%	60,78%	60,78%	58,82%	56,86%	50,98%	39,22%	31,37%	9,80%

Figure 1. Detection and Protection results in percentages against Fileless Attacks

Horizontal lines on Figure 2 represent maximum amount of points possible to reach by product in Detection and Protection parts independently.

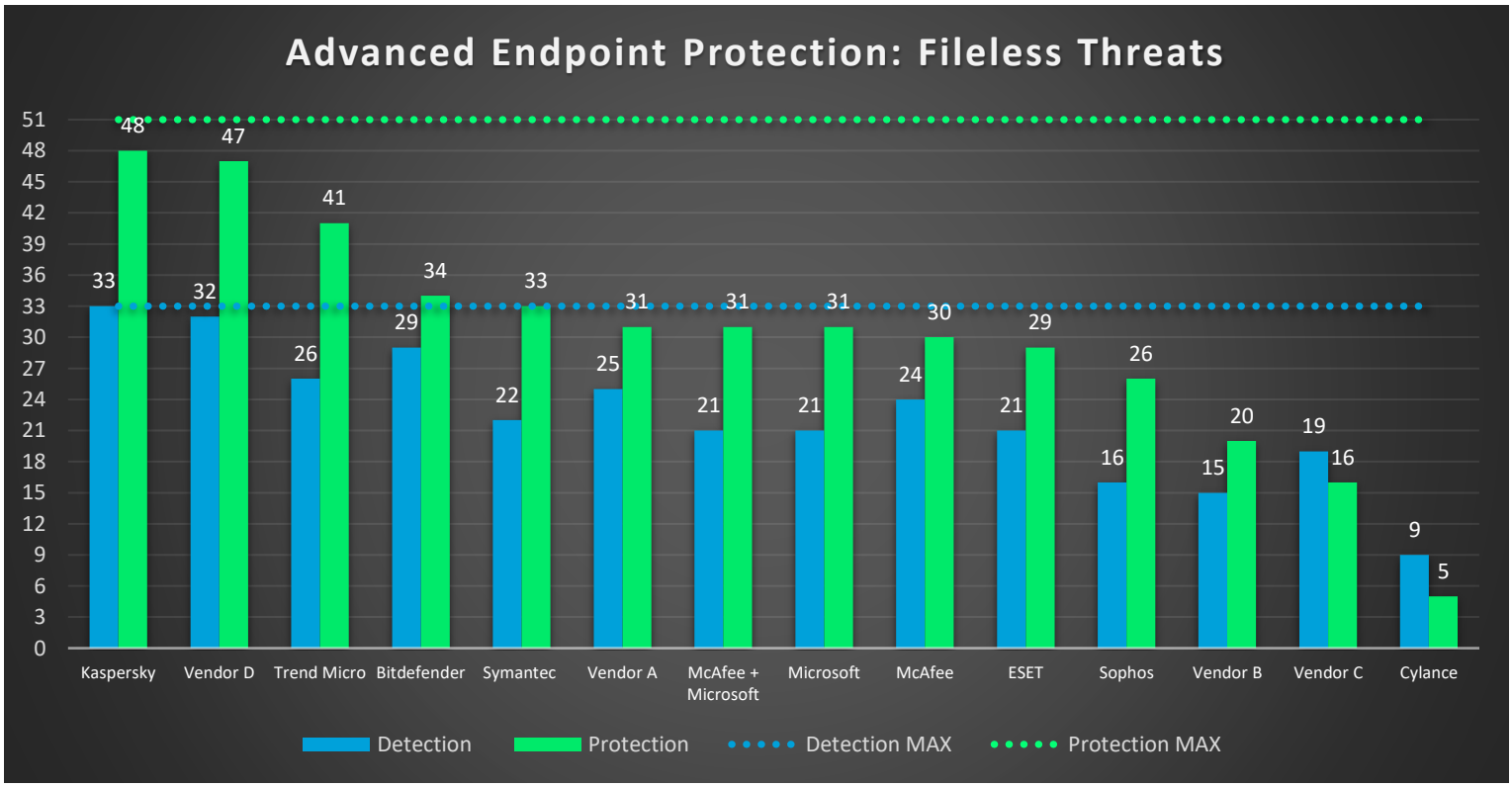


Figure 2. Detection of 33 Fileless Attacks and Protection against 51 actions

Only Kaspersky managed to detect all 33 attacks. A few other products also managed to detect a fair number of the test cases.

No product was able to protect against all 51 actions carried out during all test cases execution. Kaspersky reached the best result though, 48 points out of 51 maximum possible.

The following graphs show distribution of Detection and Protection Rates within separate four groups of test cases.

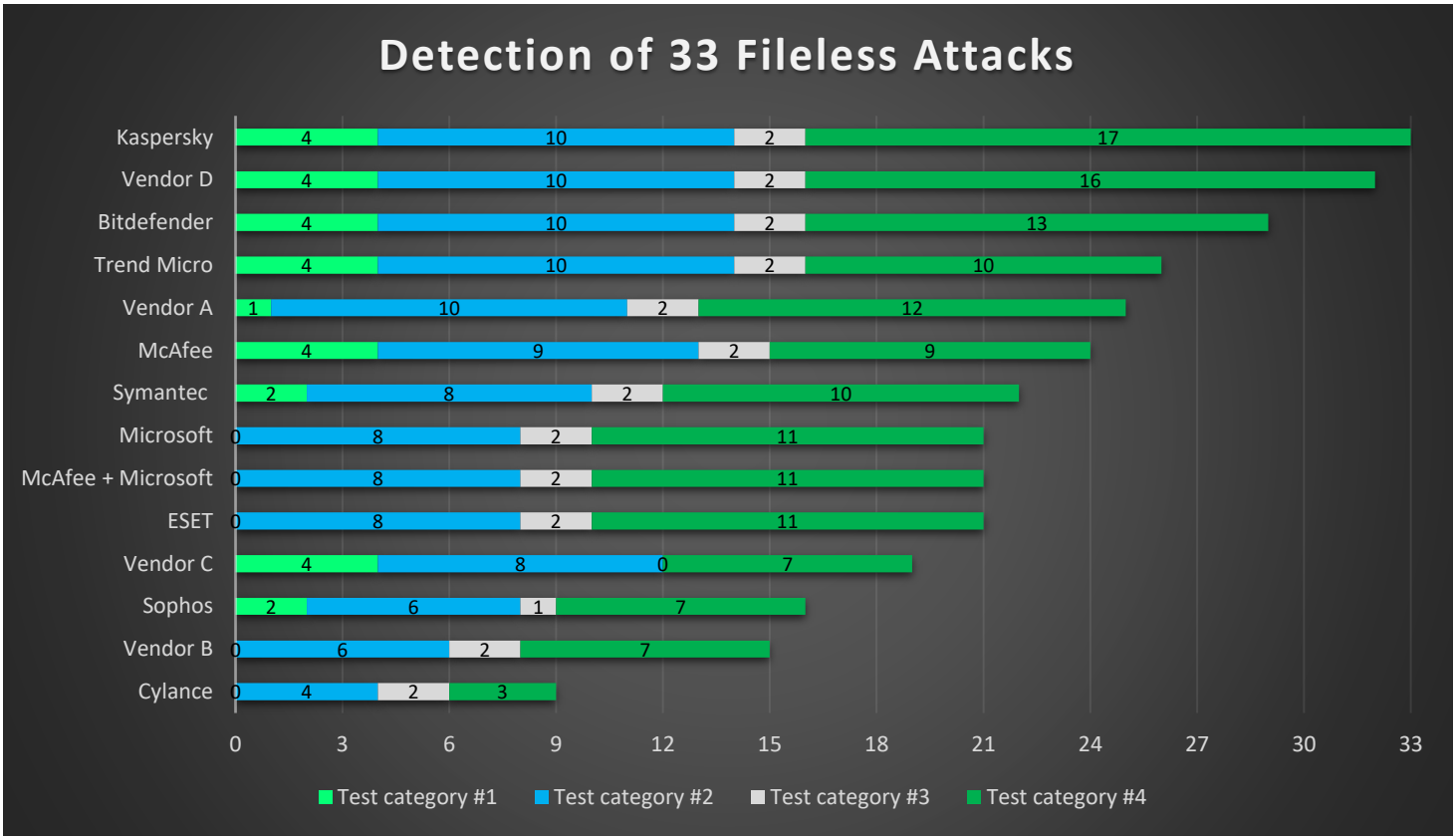


Figure 3. Distribution of Detection within four groups of Fileless Attacks

Figure 3 shows distribution of Detection within separate four groups of test cases, and sorted by total amount of Detected test-cases. Maximum scores possible for the groups are 4, 10, 2 and 17 correspondingly.

In Category #1 there are several products which alerted on all 4 test cases: Bitdefender, Kaspersky, McAfee, Trend Micro, Vendor D and Vendor C.

In Category #2 there are several products which alerted on all 10 test cases: Bitdefender, Kaspersky, Trend Micro, Vendor A and Vendor D.

Category #3 with two test cases no problem for most of the products.

In Category #4 there is only Kaspersky's product which alerted on all 17 test cases.

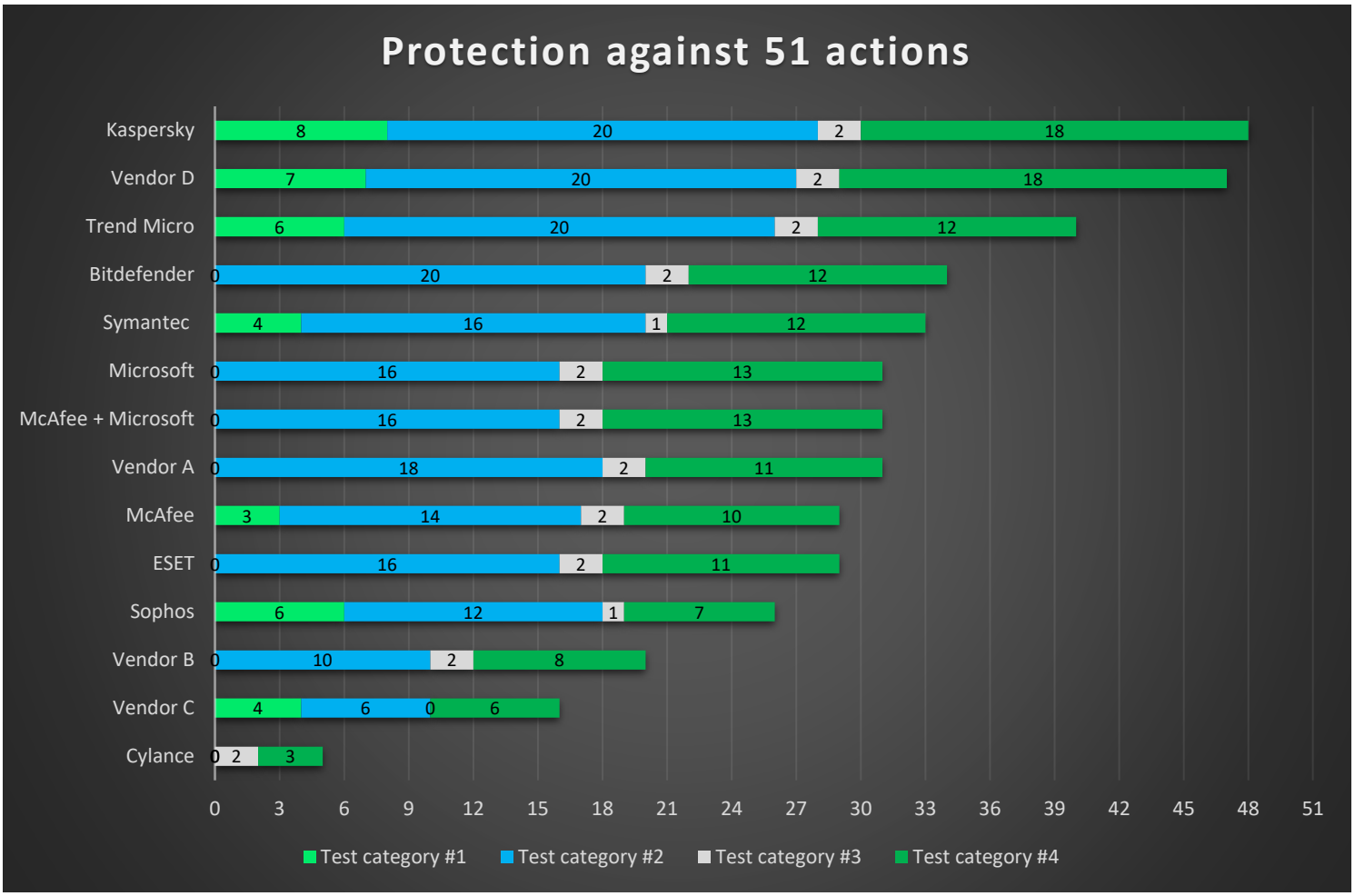


Figure 4. Distribution of Protection against malicious actions within four groups of Fileless Attacks

Figure 4 shows distribution of Protection within separate four groups of test cases, sorted by total amount of Protected actions. Maximum scores possible are 10, 20, 2 and 19 correspondingly.

In Category #1 there is no product capable to prevent all the malicious actions used in the test cases, 10 total. Kaspersky reached maximum among other participants: 8 points.

In Category #2 there are several products capable prevent all the malicious actions used in the test cases, 20 in total: Bitdefender, Kaspersky, Trend Micro, Vendor D.

Category #3 with two test cases no problem for most of the products

In Category #4 there is no product capable to prevent all the malicious actions used in the test cases, 19 total. Kaspersky and Vendor D reached maximum among other participants: 18 points.

Test Results: False Positive

The final part was a false positive test with three different test cases. It was expected that no detection of the AV products occurs and that none of the actions would be blocked. There were only three products where such false detections or blocks could be observed.

Product Name	False Detection (out of 3)	False Block (out of 1)
Bitdefender Business Security	0	0
Cylance Protect	0	1
ESET Endpoint Security	1	1
Kaspersky Endpoint Security for Business	0	0
McAfee EP Security	0	0
McAfee Mvision + Microsoft Defender	0	0
Microsoft Defender Antivirus	0	0
Sophos Central Endpoint	1	0
Symantec Endpoint Protection	0	0
Trend Micro Endpoint Apex	0	0
Vendor A	0	0
Vendor B	0	0
Vendor C	0	0
Vendor D	0	0

Figure 5. False Positives

Summary

The test results reveal the real abilities of 14 security products available on the market to detect and protect from fileless attacks. Only two products finished with near perfect scores.

However, there are also products that don't seem to focus their technology stack on protection from these techniques yet. As these were not live malware samples, those vendors may argue that they would rather add a dedicated detection for such attacks once they appear instead of a generic detection. While this will certainly work it may leave a gap until this protection is actually developed and deployed, whilst end-users remain unprotected.

There were also products that did have configuration options to completely block the execution of scripts. This would effectively prevent some of the tested fileless attacks, but would also generate false positives by preventing all legitimate uses of scripts and cause significant IT expenses for maintaining exclusion configurations. Therefore these options have not been enabled for this test.

Kaspersky integrated technology Adaptive Anomaly Control into the latest version of the product, to automatically selectively turn on blocking of potentially malicious actions, including scripts on hosts where it is necessary without causing False Positives. This option was not included into the assessment so all products remained in the same condition. Despite this, Kaspersky Endpoint Security finished with the highest scores of Detection (100%) and Protection (94.12%) among all participants.