Sophos Endpoint Security Versus Cylance CylancePROTECT Comparative Analysis 2016 June

Table of Contents

1 Introduction

MRG Effitas is a testing and research organization that specializes in specific tests. For example, our Online Banking/Browser Security tests focus on all the dangers users face when they conduct online purchases or banking transactions.

MRG Effitas has also developed a 360 Protection Test that utilizes a unique scenario where we not only focus on detection capabilities of security products, but also on the time needed to detect and neutralize samples that were capable of bypassing those security products.

MRG Effitas also conducts exploit protection testing, APT protection testing, and Performance testing.

Sophos commissioned MRG Effitas for a comparative analysis of its Sophos Endpoint Security and Control product versus Cylance CylancePROTECT. The methodology was not influenced by Sophos in any way. Sophos never suggested any changes in the policy, and there was no fine-tuning of options. The only non-default setting in the test actually lowered Sophos security default settings (see 2.1 for details).

1.1 Sophos Endpoint Security and Control

"Sophos Endpoint Security and Control is a next-generation endpoint protection. It includes malicious traffic detection, behavioral analytics, and web security. It prevents infection, detects compromised systems and remediates threats with real-time threat intelligence from SophosLabs. Web, application, device, and data control for comprehensive policy enforcement within the endpoint is included. It also includes cloud management capabilities." https://www.sophos.com/en-us/products/endpoint-antivirus.aspx

1.2 Cylance CylancePROTECT

"Cylance CylancePROTECT is a next-generation, signature-less endpoint security tool. By taking a mathematical approach to malware identification utilizing patent-pending, machine learning techniques instead of reactive signatures and sandboxes, CylancePROTECT renders new malware, viruses, bots and unknown future variants useless." CylancePROTECT also has cloud management capabilities.

https://cdn2.hubspot.net/hubfs/270968/All_Web_Assets/Data_Sheets/CylancePROTECT.pdf?t=1464899148013

1.3 Executive Summary

The purpose of this report is to run a comprehensive comparative assessment of two enterprise endpoint protection products: Sophos Endpoint Security and Control and CylancePROTECT.

In this assessment we used three tests: in-the-wild real-time protection, performance, and false-positive tests.

Final Results

Based on the number of different tests, Sophos Endpoint Security and Control performed better in the real-time protection and false-positive tests compared to CylancePROTECT. The performance results were the same for Sophos and CylancePROTECT.

2 Tests Employed

It is no secret that when it comes to malware, vendors have a lot of work on their hands. Bad guys use various techniques to evade detection. Luckily, so far antivirus developers have been able to respond to these "enhancements" swiftly.

All tests were done in a combination of Windows 7 64-bit and Windows 10 64-bit environments. The VirtualBox host and guest system for the test has been hardened in a way that common virtualization and sandbox detection techniques cannot detect the system as a test system.

The tested version of Sophos Endpoint Security and Control was Spectrum 0.4, and that of CylancePROTECT 1.2.1370.99. The test was carried out between May 24 and June 3, 2016.

2.1 High-Level Overview of the Tests

In order to gain better insight into the functionalities of Sophos Endpoint Security and Control and CylancePROTECT, we employed a combination of in-the-wild malware test (real-time protection), false-positive, and performance tests.

During the tests, we used a default install for the products. In order to test Sophos in a real-world scenario, the warning page for downloading EXE files has been turned off by policy.

2.2 In-the-Wild Malware Real Time Protection Test

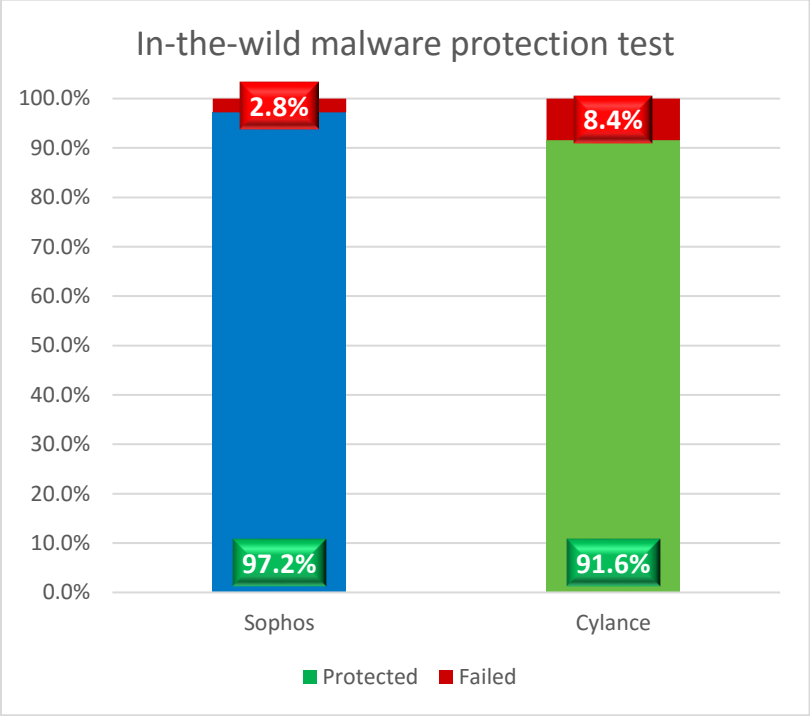
Sample selection is of fundamental importance to this and all similar tests. All samples used were "live" and "in the wild," by which we mean that they reside at the URLs selected or created by the cybercriminals, and not from a time lagged ITW list. As these are live ITW samples, they represent current zero day threats that can create an issue with sample verification. There is no effective and reliable way to verify samples before testing that does not introduce possible artificial sample submission or delay, so all verification is conducted after testing. Tests performed using samples that are later proven to be invalid are excluded from the results. MRG Effitas selects the type of samples used based on a mixture of criteria, looking at key relevancies:

1. Prevalence: they are widespread and so represent the most common threats.
2. Growth: they may be few now, but our research shows they are rapidly expanding.
3. Innovation: they employ innovative techniques to counter security measures.

We collected live samples of in-the-wild financial malware, ransomware, PUA, and rootkits, and started the malware on an already protected system. We used 214 samples in total.

Our test uses the latest and freshest samples for testing. Compared to other tests, the age of the samples we use can be measured in hours instead of days or weeks.

Result of the test



Sophos Endpoint Security and Control clearly won this test compared to CylancePROTECT.

It is important to note that CylancePROTECT does not have the typical, behavior-based (or sometimes called HIPS), post-infection detection, so malicious activity won't be detected when the malware successfully bypassed the first scan. Also due to "signature-less, update-less" mechanism, infected hosts will remain infected for a long time. The typical activities which might be detected and blocked by AV "behavior" protection:

- Persistence (Autoruns)
- Outbound communication
- Inbound communication
- Process injection
- Critical system file/configuration modification (e.g. hosts file)
- Keylogger
- Critical API hooking (rootkits, information stealers)
- Mass file encryption

During the test, we have not validated what kind of behavior protections are in place in the products. The previous information is based on information acquired from the official websites.

In this test, Cylance missed the following samples:

- 5 ransomware
- 4 Trojans
- 2 startpage
- 3 Adware
- 1 PUA
- 1 WebToolbar
- 1 Backdoor
- 1 Keylogger

In this test, Sophos missed the following samples:

- 2 Trojan
- 1 Adware
- 1 Ransomware
- 1 WebToolbar
- 1 Generic

2.3 False Positive Test

155 different applications listed either as top downloads or as new/recommended downloads from various download portals are used in the false positive test. The applications were downloaded on a different machine, packed into a single compressed file, copied to the target machine and started.

The duty of security products is to protect against malicious sites/files, not to censor or limit the access only to well-known popular applications. If the user deliberately chooses a high security setting, which warns that it may block some legitimate sites or files, then this may be considered acceptable. However, we do not regard it to be acceptable as a default setting, where the user has not been warned. As the test is done at points in time and false positives on very popular software/websites are usually noticed and fixed within a few hours, it would be surprising to encounter false positives with very popular applications. Due to this, false positive tests which are done, for example, only with very popular applications, or which use only the top 50 files from whitelisted/monitored download portals, would be a waste of time and resources. Users do not care whether they are infected by malware that affects only them, just as they do not care if the false positive count affects only them. While it is preferable that FPs do not affect many users, it should be the goal to avoid having any false positives and to protect against any malicious files, no matter how many users are affected or targeted. Prevalence of false positives based on user-base data is of interest for internal QA testing of antivirus vendors, but for the ordinary user it is important to know how accurately its product distinguishes between clean and malicious files.

The results of the false positive test is the following:

- Sophos blocked zero sample, thus it scored 100% on this test.
- Cylance blocked one sample, a security software called Hijackthis.

Our conclusion is that the difference is in the measure error rate.

2.3.1 False Positive Test – Packer Test

We created another special false positive test. The reason for this is that it is very hard to do false positive tests with "enterprise files." Most false positive tests use software targeted for the home user, and our previous test is no different. But what we often see in enterprises is that custom made software is protected with a packer to protect intellectual property. In this test, we used the totally **clean calc.exe** from Windows, and packed it with different packers. Some packers are mostly used to pack legitimate files, other packers are mostly used to pack malicious files, and there are some used to pack both legitimate and malicious files.

Packer used to pack calc.exe	**Sophos**	**Cylance**
Themida taggant	allowed	blocked
Themida no taggant	allowed	blocked
Aspack paid version	allowed	allowed
Obsidium demo	allowed	blocked
UPX	allowed	blocked
Winrar SFX	allowed	blocked
Winzip SFX	allowed	allowed
7z SFX	allowed	allowed
Hyperion	blocked	blocked

Packers work like a double-edged sword. They can be used for both good and malicious purposes. Some traditional antivirus systems are having a hard time detecting packed malware. Although antivirus can detect the presence of the packer, due to high false positives, the malware is not blocked.

But based on the results, our assumption is that **Cylance cannot differentiate between packed malware and packed legitimate files**. We would like to hear a technical explanation from Cylance as to how they can differentiate between malware and legitimate files if they are packed with the same packer, and prove us wrong. In order to detect more malicious files, Cylance sacrifices the false-positive rate for better detection. This means that companies where the custom-developed files are rarely changing, and average users are not allowed to download new files, this high false positive ratio can be accepted, with proper testing and change management in place. But in a more dynamic environment, identifying packed files blindly as malicious can cause high additional administrative overhead.

Based on the results, our opinion is that blocking files packed by UPX, WinRAR SFX or Themida with taggant information is not a proper protection mechanism.

2.3.2 Taggant Information

The problem with packers is not new. There is an IEEE standard in place to solve this problem (see https://standards.ieee.org/develop/indconn/icsg/taggant.pdf). The main idea is to embed the customer information in the packed executable, like a digital signature. Only paid versions of packers can use this taggant information. By default, security systems should check the authenticity of this taggant information, and if it is trusted, the system should allow the execution of these files. Whenever manual analysis reveals that these tagged files are malicious, the customer can be put on a non-trusted issuer list, like a black-list.

Our opinion is that antivirus and next-gen antivirus vendors should implement this standard better, as nowadays this taggant information is rarely checked by security software.

3 Performance Test

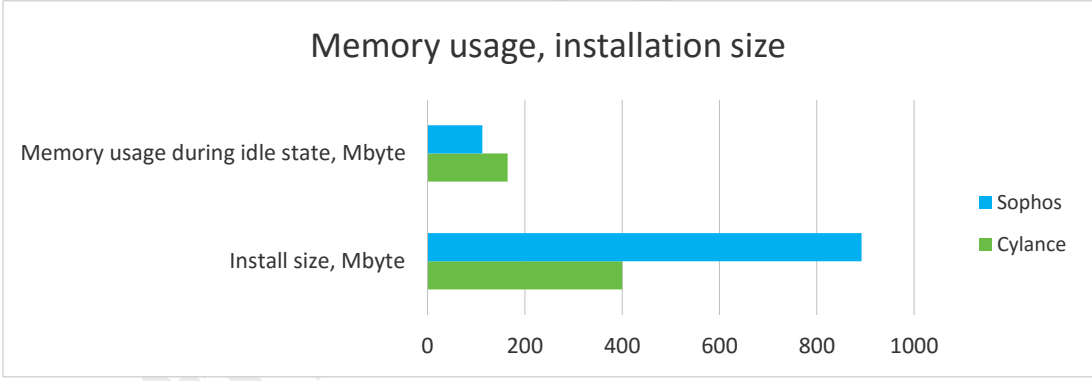
We measured the following parameters:

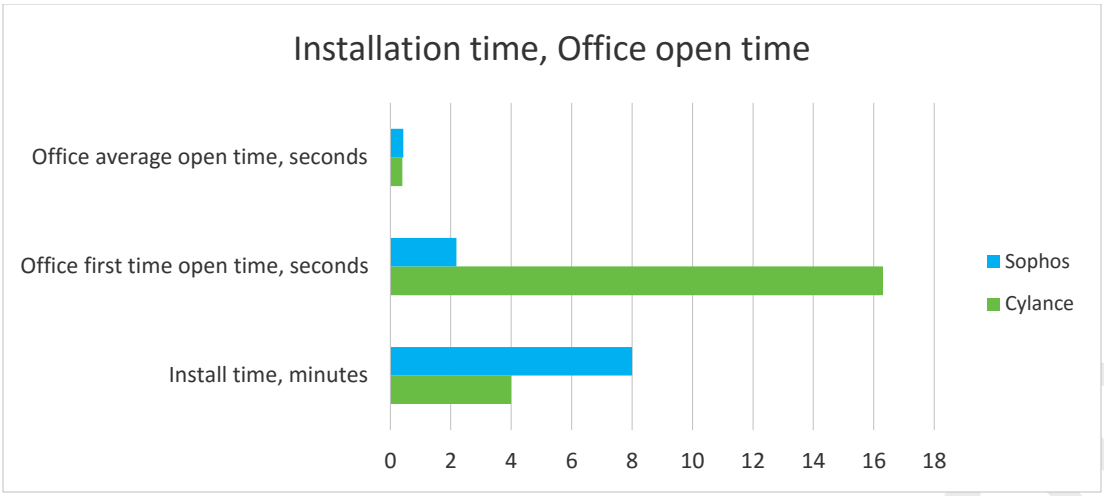
- Install time (in minutes). The install time includes finding the install webpage, registering (optional), accessing the web console, downloading, and installing the agent. The test is finished when the protection on the OS is updated, and up and running.
- Install size on the disk (program files (x86), program files, program data), in Mbyte.
- CPU utilization during idle state.
- CPU utilization during quick scan.
- Memory usage during idle state (private bytes).
- Open Microsoft Office Word 10 times, measure average.

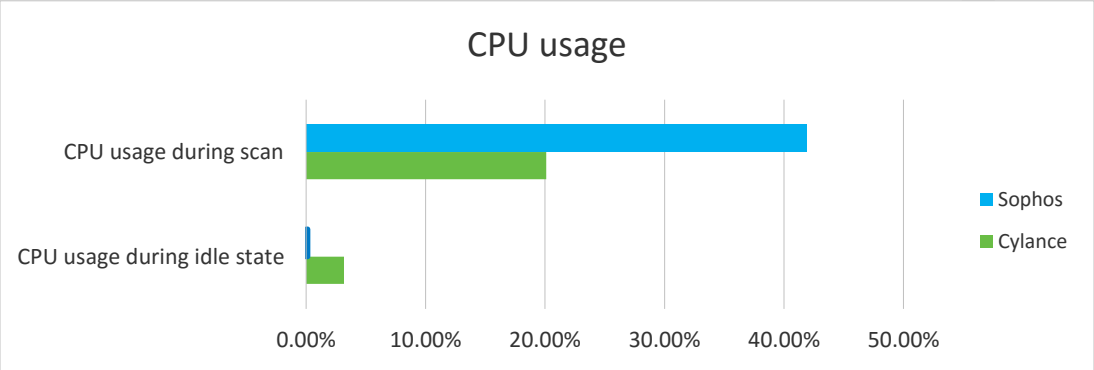
Test Results

In the following table, the color green means that the product performed better and the color red that it performed worse than the competitor.

	Cylance	Sophos
Install size, Mbyte	**400**	**892**
Memory usage during idle state, Mbyte	**165**	**113**
Install time, minutes	**4**	**8**
Office first time open time, seconds	**16.3**	**2.19**
Office average open time, seconds	**0.4**	**0.43**
CPU usage during idle state	**3.16%**	**0.13%**
CPU usage during scan	**20.09%**	**41.94%**







Cylance won three tests and Sophos won three tests, and another test resulted in a draw. Based on these results, our conclusion is that the performance on average is the same for the two product.

4 Conclusion

Based on the number of different tests, Sophos Endpoint Security and Control performed better in the real-time protection, and false-positive, tests compared to CylancePROTECT. The performance test results were the same for Sophos and CylancePROTECT.

5 Appendix

5.1 Methodology Used in the "In-the-Wild Test"

1. Windows 7 Ultimate Service Pack 1 64 bit and Windows 10 64-bit operating systems are installed on a virtual machine, all updates are applied and third party applications installed and updated according to our "Average Endpoint Specification."[1]
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications to be used in the test.
4. An individual security application is installed using default settings on each of the systems created in step 2 and then, where applicable, it is updated and shut down. If the installer has the option to participate in cloud protection, PUA protection, or browser extensions, all of these are enabled.
5. Testing is conducted by:
    a. Downloading the sample using Internet Explorer to the desktop. The browser is kept running, and then the sample is executed.
6. A test is deemed to have been passed based on the following criteria:
    a. The security application blocks the URL where the sample is located, thus preventing its download.
    b. The security application detects the sample while it is being downloaded to the desktop.
    c. The security application detects the sample when it is executed according to the following criteria:
        i. It identifies the sample as being malicious and either automatically blocks it or pauses its execution, advises the user not to execute it and awaits user input.
7. A test is deemed to have been failed based on the following criterion:
    a. The security application fails to detect the sample under condition 6a, 6b or 6c.
8. Testing is conducted with all systems having internet access.
9. Each individual test for each security application is performed from a unique IP address. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.

[1] Latest Microsoft Office and Adobe Flash Player is installed, SmartScreen protections are turned off, Microsoft Defender is turned off, UAC is turned off