Symantec Endpoint Protection Cloud Cross-platform Protection Test

Date of the report: November 16rd, 2016, last update January 26th, 2017

Executive Summary

In November 2016, AV-Test performed a test of Symantec's Endpoint Protection Cloud (SEP Cloud). SEP Cloud is a comprehensive protection solution for environments where the security of diverse devices and platforms must be guaranteed, with the ease of management from a single cloud-based management console.

The presented evaluation assesses SEP Cloud's protection capacities on three current operating systems: Windows, Mac OS Sierra and Android. In a laboratory setting that emulated realistic working conditions, each of the platform-specific instantiations of SEP Cloud was confronted with a set of current malware samples. During the test the detection rates and removal performance were recorded. For the Windows operating system, the evaluation comprised an additional performance test – the assessment of the software's influence on the overall system's response time to commonplace working activities.

SEP Cloud delivered close-to-perfect results on all platforms. It scored a full 100% of successful detections on Windows and Android systems, and a convincing 95.92% on Mac OS. Furthermore, the software had relatively small impact on Windows system performance, scoring 5.5 out of 6 points in our performance testing.

Overview

Important changes in everyday working environments have occurred in recent years. The time where an employee's work was done at one desk, using a single desktop computer are long gone. Laptops, tablets, and smart phones allow employees to be responsive and productive wherever, whenever they choose. Technological advances have not only had an important impact on *how* work and leisure time is organized– but also on the landscape of cyber threats.

Mobile platforms in particular have become a major target in recent years. In 2011, AV-Test received more than 9,000 new malware samples for the Android platform. Since then, this number has increased exponentially, with over 4,000,000 new samples in 2014. Figure 1 displays the amount of Android malware samples collected each year since 2011. Currently, AV-Test's malware database contains more than 16 million malware samples solely for the Android platform.

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

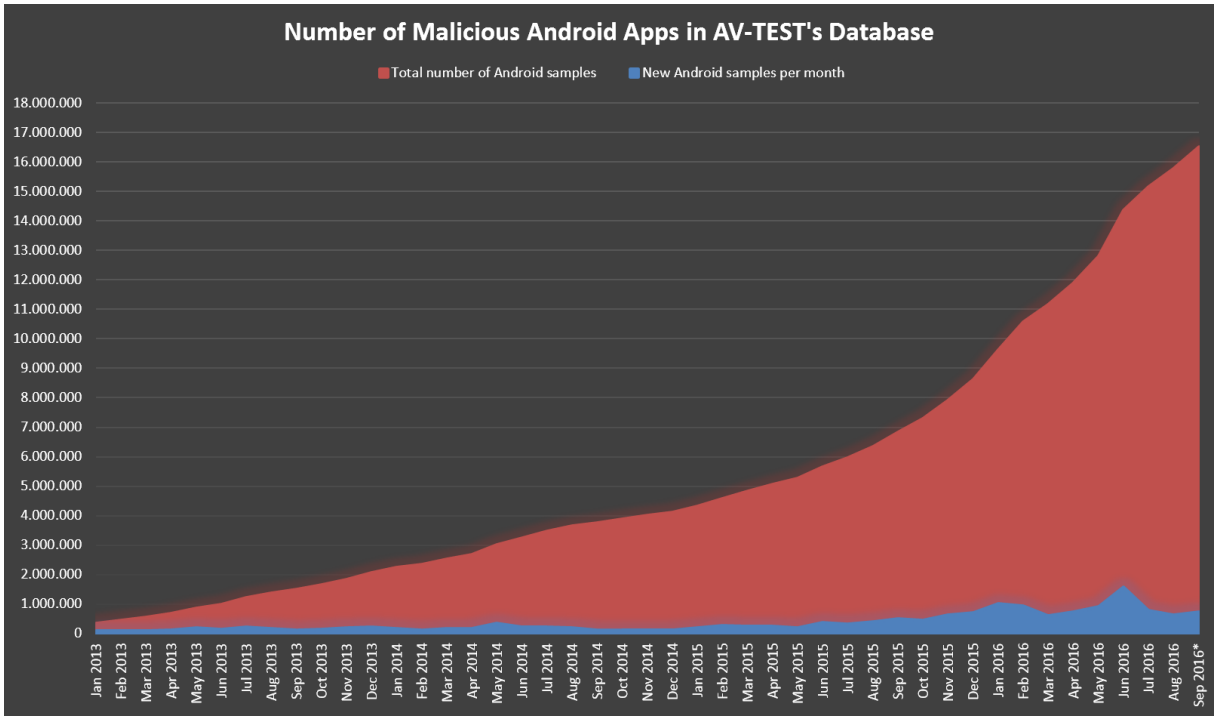

Figure 1: New android samples added per year

The situation is similar on other operating platforms. In the year 2000, AV-Test received more than 170,000 new samples across all operating platforms. By 2013 the number of new samples grew to over 80,000,000; and has continued to grow through 2016. The growth of these numbers is displayed in Figure 2. AV-TEST currently has over 590 million malware samples in its database.

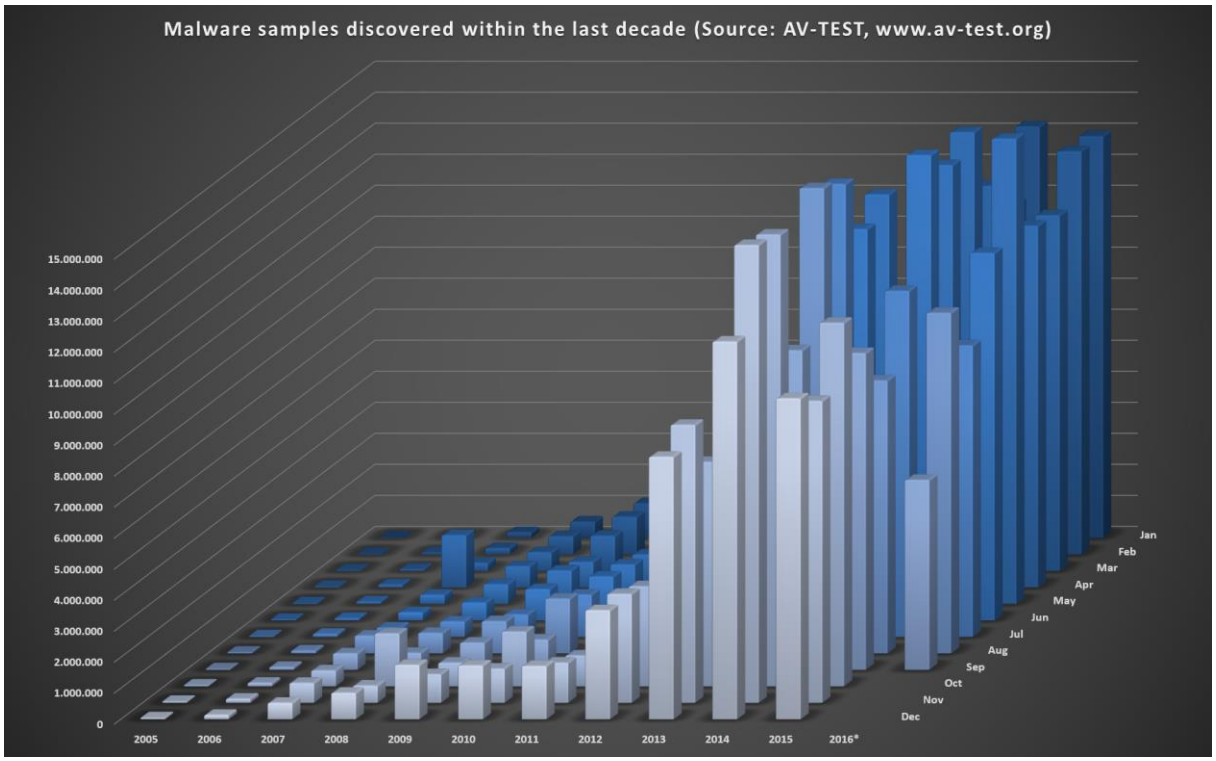

Figure 2: Malware samples overview

With the continued growth and sophistication of new malware, modern businesses need a comprehensive, all-encompassing security strategy; regardless of their size. Employees must be

provided with solutions that support their preferred working environments to foster productivity and avoid the security risks entailed by the new working reality.

With SEP Cloud, Symantec provides a solution to address the needs of the modern business. It offers cloud-based threat detection for the commonly used operating platforms: Windows, Mac OS and Android systems. In November 2016, Symantec commissioned a test at the AV-Test laboratories to prove the comprehensive protection performance of their software solutions. This report sums up the results of the performed protection and performance tests.

Methodology and Scoring

Tested products

The presented tests were performed in November 2016. They all featured the latest available product releases at the time of the test:

(1) **Windows:** Symantec Endpoint Protection Cloud, v22.6.4.5
(2) **Mac OS:** Symantec Endpoint Protection Cloud, v7.2 (Build 90)
(3) **Android:** SEP Cloud (with Symantec Norton Mobile Security 3.15)

Platforms

All tests were performed on actual physical machines. No Virtual Machines were used. All tests for a defined operating system were carried out on devices with identical hardware configurations as described below.

Windows

All tests for the Windows operating system were performed on identical PCs equipped with the hardware specified in the Appendix. The detection tests were performed on the Windows 7 platform. The performance test used the same Windows 7 system and additionally a Windows 10 platform. In both cases, all patches available on October 1st 2016 were previously installed.

Mac OS

All tests for the Mac OS operating system were performed on identical computers equipped with the hardware specified in the Appendix. The operating system was Mac OS Sierra 10.12.

Android

Prevalence Tests

The prevalence tests were performed on identical Nexus 5 devices with the hardware specified in the Appendix. The operating system was Android 5.1.1 build number LMY48M.

Real-time Tests

The real-time tests were performed on identical Motorola Moto G (2. Gen.) devices with the hardware specified in the Appendix. The operating system was Android 5.0.2 build number LXB22.99-16.3.

Testing Approach

There are a few generic principles that were followed no matter the considered operating system:

(1) **Physical Devices**. The test devices used were physical devices. No Virtual Machines were used.
(2) **Product Cloud/Internet Connection**. The Internet was available to all tested products that used the cloud as part of their protection strategy.
(3) **Product Configuration**. All products were run with their default, out-of-the-box configuration.
(4) **Clean device for the start of the test**. The test devices were restored to a clean state before testing the malware samples.
(5) **Sample Cloud/Internet Accessibility.** If the malware used the cloud/Internet connection to reach other sites in order to download other files and infect the system, care was taken to make sure that the cloud access was available to the malware sample in a **safe** way such that the testing network was not under the threat of getting infected.

For the Android platform, this set was extended by some platform-dependent principles:

(6) **No rooted devices for the test.** Android devices were not rooted and or in any other way tampered with.
(7) **Sample execution on Android**. Samples were only installed and not launched, because of the lack of restore function after each sample.

Windows

Real-World Test

The real-world test evaluated the security product's protection performance against current, in-the-wild malware samples. The samples were derived from a diverse set of download domains, no two URLs in the test set originated from the same second-level domain. The sample was brought to the testing environment on its natural introduction vector – samples collected as email attachments were sent to the test computer as email messages, web-based threats were downloaded to the target systems from an external web server. The natural activity flow of a normal user was simulated as closely as possible, e.g. by following a certain, typical chain of URLs leading to an infection.

To allow the sample to execute its malicious potential, it was allowed to run undisturbed for 3 minutes. During this time period, the malware may initiate connections to other systems on the internet to install itself to survive a reboot (as may be the case with certain key-logging Trojans that only activate fully when the victim is performing a certain task).

Subsequently, the impact of the malicious threats and the ability of the product to detect them was evaluated in a consistent and systematic manner. For each test sample, the detection success of the security product was noted and protocoled, allowing three possible outcomes:

a. **Successful blocking of the threat.** The method of notification/alert was noted, including any possible required user interventions. If the solution required an intervention, the prompted default behavior was chosen. Any additional downloads were noted. The blocking was noted as successful if the malware was kept from causing an infection to the target system.
b. **Successful neutralization of the threat.** The notification/alert was noted as stated before, default user interventions were chosen. Successful neutralization should not have included additional downloads. It was assessed whether all aspects of the threat were completely removed (or if the neutralization was limited to *active* aspects of the threat).
c. **Threat compromises the machine.** The malware successfully harmed the target system despite the installed security product. Information about the non-detected threat aspects were noted.

False positive test

Security software can use a variety of techniques to protect the user's working environment. However, if a product's detection mechanisms are too sensitive, the software can disturb normal working activities with continuous warnings. The number of unjustified alarms raised by a security product is tested in *false-positive testing*.

The false positive test used a set of legitimate software files that were likely to trigger detection due to their composition and behavior. The software was downloaded from the official websites and installed on the systems. It was executed and tested to establish that is was functioning correctly. False alarms were documented using the software's detection logs and screenshots.

Performance test

The performance test examined the product's impact on system performance in typical daily use. It compared the system's response time with and without the product being installed. For testing, five typical tasks were identified that were likely to be performed by a user on a daily basis:

1. Downloading files from the Internet: In order to ensure equivalent conditions for all products, the files were downloaded using a server in a separate test network.

2. Launching websites: For this test, a few dozen websites were loaded, e.g. Amazon, Yahoo, Apple and Google. The test set consisted of highly available websites to ensure a fair comparison.

3. Installing applications: In this test, applications were installed per command line (without clicks), and the time was clocked for this operation. Included in this test section were popular programs such as Flash Player and Adobe Reader.

4. Opening applications, including a file: In this test, a DOC file, a pdf file and a presentation file – all having a large size – were opened repeatedly and directly with LibreOffice.

5. Copying files: Security solutions can impact performance and frustrate users, especially when copying data in Windows. To gauge the impact, the lab team examined how heavily the products delayed the copying of files. The test featured a 3.3 GB set with a wide variety of file types such as films, images, graphics, documents, pdfs and programs.

To ensure that no other processes or scheduled tasks influenced the measurement we disabled automatic updates of Windows and of the products themselves. Also, all scheduled scans of the tested products were deactivated. Additionally, we waited a predefined time before we started the test and made sure that all services for Windows and the products were running.

Mac OS

For each test, the considered security product was installed on an up-to-date Mac OS platform. Subsequently, the software was updated and the resulting version number cross-checked to the ones noted on the manufacturer's websites. Only products downloaded from the AV vendor's official web platform was used for testing, as the versions provided by the Mac App Store might have contained limited functionality.

The basis of testing was a set of Mac OS-specific malware samples, assembled during the recent months. The sample set contained typical formats of malware distribution, such as archive files (e.g. DMG and PKG) and executables. The test set was designed to ensure it included a variety of prevalent malware families.

For testing, the malware samples were transferred to the testing environment. Subsequently, an on-demand scan of the system was launched. The tester noted successful detections and misses using software logs and screenshots.

Android

On the Android platform, two types of tests were performed: The *prevalence test* evaluated the product's protection performance on current malware samples, collected over the four weeks preceding the test. During *real-time testing*, the security software was confronted with newly discovered threats that were not older than 24 hours.

There were two different tests that were performed on Android devices: *on-demand scan* and *on-access scan*. In the former, the malware sample was placed on the device and the product was triggered to launch a full scan. The security software should have found the new files and provided the user with options for its neutralization. In the latter, the malware sample was installed on the Android device to test the threat monitoring of the security solution – during the installation the AV product was supposed to warn the user and provide her with options to neutralize the threat.

On the prevalent set, both tests were performed whereas the real-time test was limited to the on-access component. Further details on the testing procedure can be found in a separate report, please click here Android report.

Test Results

Windows

Protection

SEP Cloud protection produced perfect results when confronted with current Windows malware. In the test environment, the software detected 100% of the examined 54 malware attacks.

Performance

While protecting optimally from current threats, SEP Cloud had only moderate impact on system performance. The security solution caused a slow-down of 10.05% on a Windows 7 system and 10.86% on Windows 10 – reaching a nearly perfect score of 5.5 out of 6 points.

Looking at the results in more detail, it was the task “Install applications” that caused performance losses across all analyzed platforms and test sets (with a response time increase of about 20%). In contrast, SEP Cloud had only minimal impact on the time necessary to perform a download (between 0.36% and 3.14%).

Mac OS

On the Mac OS platform, SEP Cloud scored 95.92% by correctly detecting 47 of 49 malware samples. The security software performed well to perfectly on nearly all malware categories; the overall result was somewhat hampered by an 83.3% detection rate on scripted malware samples.

Android

Prevalent Test

The prevalent test shows how well the security solutions were capable of detecting common threats from the past 4 weeks. SEP Cloud achieved a perfect result, successfully detecting 100% of the 3809 malware samples.

Real-Time Test

The real-time test shows how well a security solution reacts to new threats. None of the malware samples were older than 24 hours. SEP Cloud delivered close-to-perfect results, detecting 99.49% of the 3139 up-to-date malware samples.

Conclusion

With its ability to protect across diverse devices and platforms, Symantec provides a comprehensive security solution easily managed through a single cloud-based console. The unified, security strategy protects company-internal work stations as well as mobile devices such as laptops, tablet PCs and smart phones running Windows, Mac OS, and Android operating systems.

The objective of the here-presented tests was to assess the products' protection performance on the diverse working platforms. Indeed, Symantec's products delivered convincing results across the tested platforms – scoring 100%-detection rates on Windows and during the Android prevalent test, and good results on Mac OS (95.42% detection rate) and during the Android real-world test (99.49%).

Threat protection may consume a considerable amount of system resources, which can lead to user dissatisfaction. Therefore, we also examined the solution's impact on system performance – by performing everyday working tasks and measuring the impact on the system's response time. SEP Cloud performed well – system response was delayed by a mere 10%, scoring a close-to-perfect 5.5 out of 6 points on all platforms tested.

On mobile platforms, the functionality of SEP Cloud extended beyond simple mobile security. The Android solution provided several additional features that simplified the work of the IT security department. It also provided several management tools: mobile device management (MDM), device health monitoring, device security policy management and access policy management. Furthermore, the package included the App Advisor, which allows users to evaluate mobile applications. The potential of the application to cause privacy issues and performance impacts was assessed. Ultimately, the cloud-based management console was found to provide the ease of management needed for the modern business and mobile workforce.

Appendix

Hardware specifications

Windows

Test type	Detection and Performance	Performance
Operating system	Windows 7 Ultimate with all patches available on October 1st 2016.	Windows 10 Professional with all patches available on October 1st 2016.
Hardware	• Intel Xeon Quad-Core X3360 CPU • 4 GB RAM • 500 GB HDD (Western Digital) • Intel Pro/1000PL (Gigabit Ethernet) NIC	• Intel i7 3770 CPU • 16 GB RAM • 512 GB SSD (Samsung) • Intel Pro/1000PL (Gigabit Ethernet) NIC

Android

Test type	Prevalent test	Real-time test
Operating system	Nexus 5 Android 5.1.1 build number LMY48M	Motorola Moto G Android 5.0.2 build number LXB22.99-16.3
Hardware	• Memory: 2GB RAM • Storage: 16GB Flash • CPU: Qualcomm Snapdragon 800, 4x2.26Ghz • GPU: Adreno 330	• Memory: 1GB RAM • Storage: 8GB Flash • CPU: Qualcomm Snapdragon 400, 4x1.2Ghz • GPU: Adreno 305

Mac OS

Operating system	Mac OS Sierra 10.12.
Hardware	• iMac 21.5 Late 2013 • 16 GB 1600 MHz DDR3 • 500GB SSD • Intel Core i5 2,7 GHz

Funding of the test

This test was commissioned by Symantec and performed by AV-Test GmbH.