Symantec Endpoint Protection Cloud Comparison Test for Android: Protection

A test commissioned by Symantec and performed by AV-Test GmbH
Date of the report: November 16rd, 2016, last update: November 23th, 2016

Executive Summary

In September 2016, AV-Test performed a comparative review of Avast Mobile Security, Avira Antivirus Security, ESET Mobile Security & Antivirus, Lookout Security and Antivirus, Qihoo 360 360 Security against Symantec Endpoint Protection Cloud (SEP Cloud) that delivers comprehensive device protection including mobile security and mobile device management (MDM) for a heterogeneous organization, to determine their prevalent and real-time prevention.

This report details only the mobile security portion of the test results. For the full report detailing protection across heterogeneous devices, please click here Full Report.

The prevalent test corpus consisted of 3809 malware samples, the real-time test corpus of 3139 malware samples. At first we started with an on-demand test, which means scanning all samples on the SD-card of the device. To perform the prevalent on-demand test, a clean Android 5.1.1 image was used on several identical LG Nexus 5 Android devices. We installed the security app on the device and pushed the samples to the SD-card and performed a scan. The result of the scan was captured as a screenshot and we let the app delete the detected samples. The not detected samples were pulled from the device and are the basis for the following on-access test.

To perform the prevalent on-access test runs, a clean Android 5.1.1 image was used on several identical Nexus 5 Android devices. On this device the security app was installed, alongside the security solution our own AV-Test Android test app was installed to recognize the detections of the product. Each malware sample that was not detected during the on-demand scan was installed on the device and any detection by the security app was recognized by screenshot and our app. After a period of time the malware sample was uninstalled from the device and we proceeded the next sample.

A simultaneous execution of the real-time test with all mentioned security solutions guaranties the best comparability of the results. The real-time test was performed using a clean Android 5.0.2 image on several identical Motorola Moto G (2. Gen.) Android devices. For this test, we used the same workflow as described in the on-access test of the prevalent test.

SEP Cloud delivered perfect results for the prevalent detection test, while the other products missed a few samples. In the real-time test, SEP Cloud and ESET Mobile Security & Antivirus delivered the best results, while the other products missed a few samples. Unfortunately, Lookout Security and Antivirus delivered an unconvincing result in both tests.

Overview

With the increasing number of threats that is being released and spreading through the Internet these days, the danger of getting infected is increasing as well. A few years back there were new malware apps released every few days. This has grown to several thousand new threats per day.

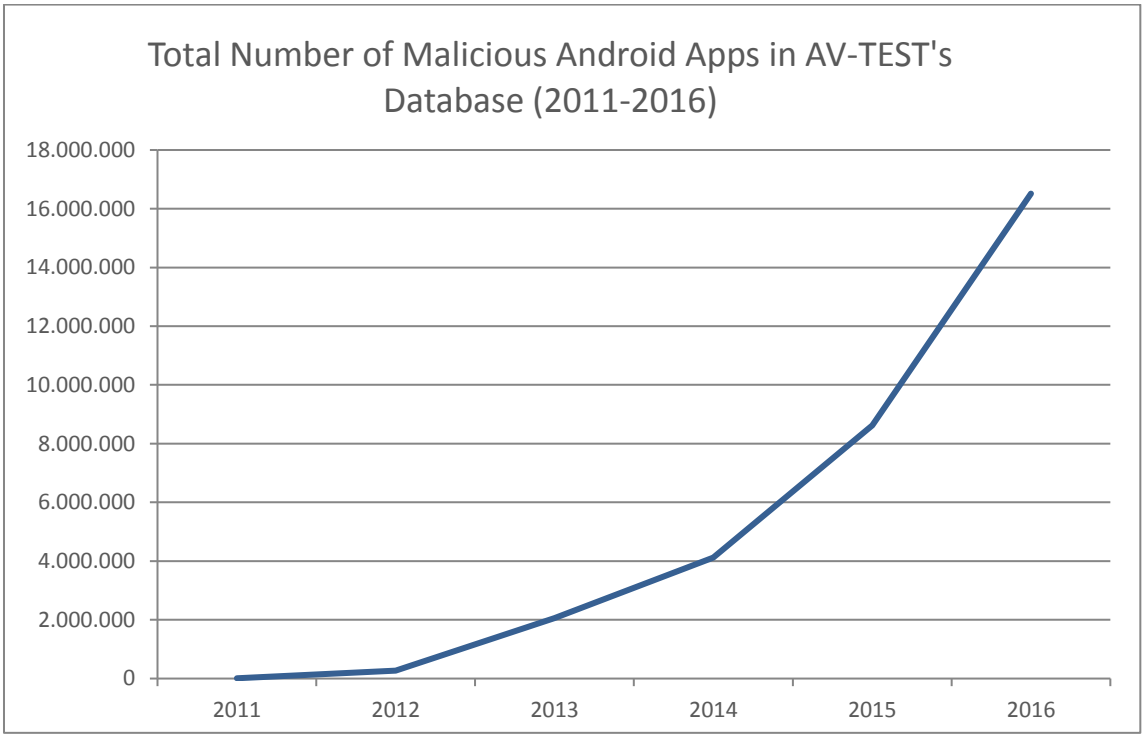

Figure 1: New android samples added per year

In the year 2011, AV-Test received more than 9,000 new samples, and in 2014, the number of new samples grew to over 4,000,000 new samples. The numbers continue to grow in the year 2016. The growth of these numbers is displayed in Figure 1. AV-TEST currently has over 16 million android malware samples in its database.

The volume of new samples that have to be processed by anti-malware vendors in order to protect their customers can cause problems. For an anti-malware product, it is not always possible to successfully protect an Android device in real-time. It is possible that an Android device can get infected, even if an up-to-date anti-malware app is installed, because signatures are provided only every few hours, which sometimes may be too late. Infections cause financial losses, either because sensitive data is stolen or because the Android device cannot be used anymore until the malware is completely removed from the system. On the other hand, more protection layers need more resources on the Android device which can cause influences in the performance.

Products Tested

The testing occurred in September 2016. AV-Test used the latest releases available at the time of the test of the following six products:

(1) Avast Mobile Security 5.4
(2) Avira Antivirus Security 4.5
(3) ESET Mobile Security & Antivirus 3.3
(4) Lookout Security and Antivirus 9.49
(5) Qihoo 360 360 Security 3.7
(6) SEP Cloud (with Symantec Norton Mobile Security 3.15)

Methodology and Scoring

Platform

LG Nexus 5

The prevalent tests have been performed on identical Nexus 5 devices with the following hardware:

- Screen: 4.95", 1920x1080 (445 ppi)
- Memory: 2GB RAM
- Storage: 16GB Flash
- CPU: Qualcomm Snapdragon 800, 4x2.26Ghz
- GPU: Adreno 330
- Wi-Fi: 802.11 a/b/g/n/ac

The operating system was Android 5.1.1 build number LMY48M

Motorola Moto G (2. Gen.)

The real-time tests have been performed on identical Motorola Moto G (2. Gen.) devices with the following hardware:

- Screen: 5.00", 1280x720 (294 ppi)
- Memory: 1GB RAM
- Storage: 8GB Flash
- CPU: Qualcomm Snapdragon 400, 4x1.2Ghz
- GPU: Adreno 305
- Wi-Fi: 802.11 a/b/g/n

The operating system was Android 5.0.2 build number LXB22.99-16.3

General Approach

1. **No rooted devices for the test.** The test devices should not be rooted and or in any other way tempered.
2. **Clean device for the start of the test**. The test devices should be restored to a clean state before testing the malware samples.
3. **Physical Devices**. The test devices used are physical devices. No Virtual Machines should be used.
4. **Product Cloud/Internet Connection**. The Internet should be available to all tested products that use the cloud as part of their protection strategy.
5. **Product Configuration**. All products should run with their default, out-of-the-box configuration.
6. **Sample execution on Android**. Samples should only be installed and not launched, because of the lack of restore function after each sample.

Prevalent Test

The prevalent test has been performed according to the methodology explained below.

The Prevalent test consists of 2 parts, on-demand scan and on-access test.

The first part of the prevalent test is the on-demand scan.

1. Push samples to the SD-card via the Android Debug Bridge
2. Start the on-demand scan of the product and wait for it to finish
3. Document the result presented by the product (e.g. by creating screenshots or storing report files)
4. Let the product delete the detected samples
5. Pull the remaining samples from the SD-card via the Android Debug Bridge

The pulled (not detected) samples are the basis for the second part of the prevalent test: the on-access test.

Device preparation:

- Install our own AV-Test Android test app alongside the security solution, to recognize the detections of the product

Test steps:

1. Check internet connectivity on the device
2. Install sample via the Android Debug Bridge
3. If there were any notifications from the anti-virus app they have been recognized and documented by our app (e.g. by creating screenshots or storing report files)
4. For documentation, take a screenshot of the device screen
5. Uninstall sample via the Android Debug Bridge
6. Press Home-Button

Repeat steps 1 to 6 for each sample.

Real-time Test

The real-time test has been performed according to the methodology explained below.

Device preparation:

- Install our own AV-Test Android test app alongside the security solution, to recognize the detections of the product

Test steps:

1. Check internet connectivity on the device
2. Install sample via the Android Debug Bridge
3. If there were any notifications from the anti-virus app they have been recognized and documented by our app (e.g. by creating screenshots or storing report files)
4. For documentation, take a screenshot of the device screen
5. Uninstall sample via the Android Debug Bridge
6. Press Home-Button

Repeat steps 1 to 7 for each sample. After test of 100 samples the devices are rebooted.

Samples

The set contained 3809 prevalent samples and 3139 real-time samples that were able to harm an Android device. The prevalent malware set contained Android malware samples, which were not older than 4 weeks. Real-time malware samples consisted of Android malware samples, which were first seen by within the last 24 hours.

Test Results

Prevalent Test

The prevalent test shows how well the security solutions are capable of detecting most common threads from the past 4 weeks. The following figure shows the overall score of the six tested solutions.

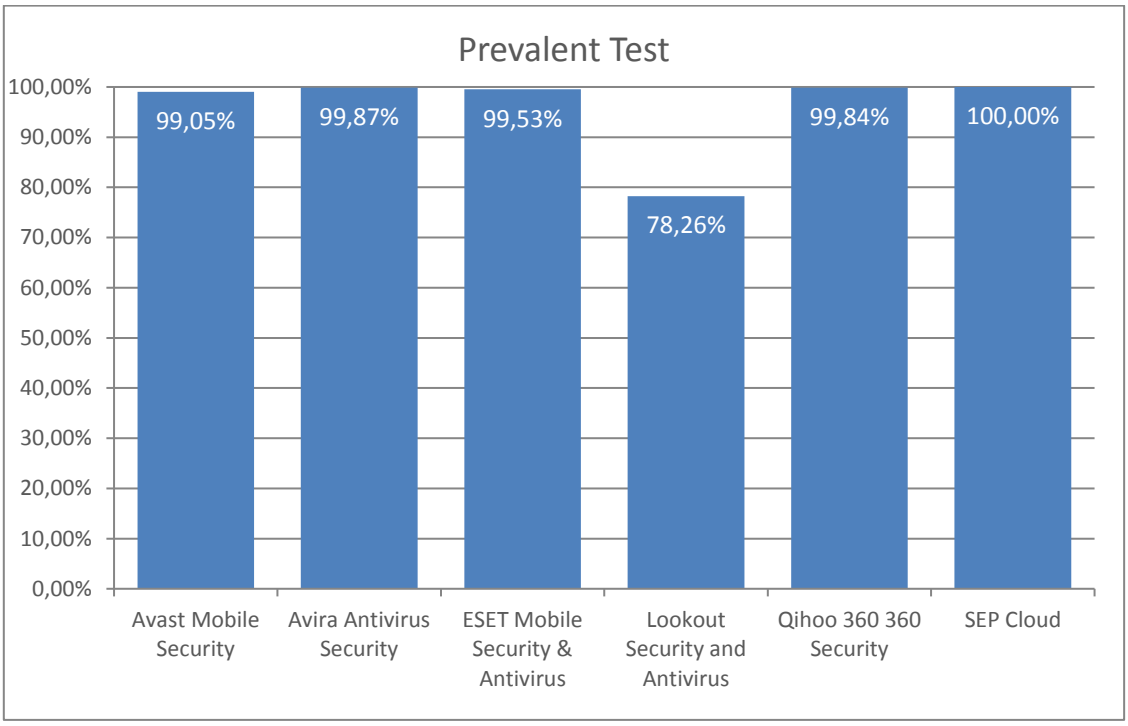

Figure 2: Prevalent Test

SEP Cloud achieved perfect results in the prevalent detection test, while the other products missed only a few samples. All other products except Lookout delivered good results for prevalent test.

Real-Time Test

This test was performed simultaneously with all 6 security apps, and shows how well a security solution reacts on new threats. The following figure shows the overall score of the six tested solutions.

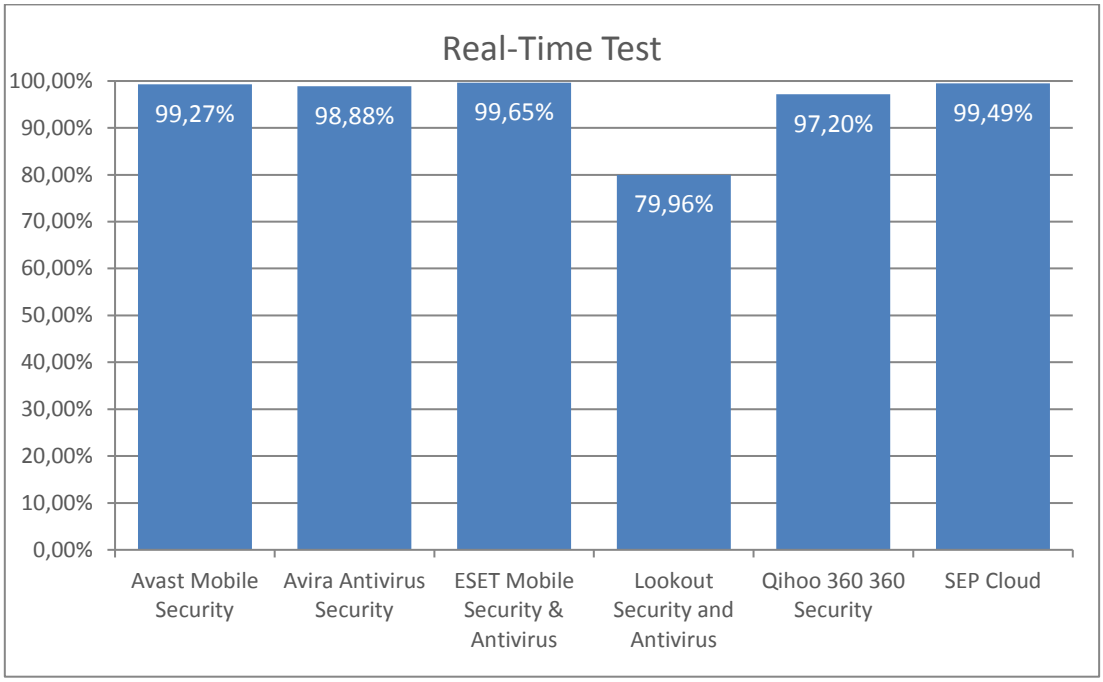

Figure 2: Real-Time Test

None of tested products was able to achieve a perfect result, but SEP Cloud and ESET Mobile Security & Antivirus delivered the best results, while the other products missed a few more samples. All other products except Lookout delivered good results.

FEATURES

All tested products provide a wide list of security features, e.g. Anti-Theft or Safe Browsing for their users.

Product	Anti-Theft (Remote-Lock / Remote-Wipe / Locate)	Call Blocker	Message Filter	Safe Browsing	Backup	Others
Avast Mobile Security	+ / + / +	+	-	+	-	App Locking, Privacy Advisor, Wi-Fi Security
Avira Antivirus Security	+ / + / +	+	-	+	-	Identity Safeguard, App Lock, Privacy Advisor, SafeSearch
ESET Mobile Security & Antivirus	+ / + / +	+	+	+	-	Security Audit
Lookout Security and Antivirus	+ / + / +	-	-	+	+	Privacy Advisor
Qihoo 360 360 Security	+ / + / +	+	+	+	-	
SEP Cloud	+ / + / +	+	-	+	+	App Advisor (incl. privacy leakage and performance impact), Device Health Management, Remote Locate (via SMS), Access Policy Management

SEP Cloud extends beyond mobile security and delivers mobile device management (MDM) for business use-cases. SEP Cloud offers functions like device health monitoring, device security policy management (lock-screen passcodes, encryption settings, restrictions) and access policy management (corporate email and Wi-Fi profiles) through the cloud console.

Appendix

Version information of the tested apps

Developer, Distributor	Product name	Android package name	Version code	Version
Avast	Mobile Security	com.avast.android.mobilesecurity	12436	5.4.1
Avira	Antivirus Security	com.avira.android	3941	4.5
ESET	Mobile Security & Antivirus	com.eset.ems2.gp	9330023	3.3.23.0
Lookout	Security and Antivirus	com.lookout	9490109	9.49.1-6e45ba4
Qihoo 360	360 Security	com.qihoo.security	2219	3.7.9.6201
Symantec	SEP Cloud	com.symantec.endpoint.ua	20160715	1.0.6041