

Anti-Virus Comparative



Mobile Security Review 2016

Language: English
September 2016

Last Revision: 25th September 2016

www.av-comparatives.org

Table of Contents



Introduction	3
Android Marshmallow	4
Security Features	6
Overview	8
Products tested	8
Protection against Android malware	10
Test Set & Test Results	11
Battery Drain Results	12
Alibaba	13
Antiy	15
Avast	16
AVG	19
Avira	21
Baidu	23
Bitdefender	25
ESET	27
G Data	30
Kaspersky Lab	33
McAfee	36
Tencent	38
Trend Micro	39
Feature List	42
Copyright and Disclaimer	43

Introduction

This report provides test reports and reviews of security products for smartphones running Google's Android operating system. All tests were run on Android 6.0.1, which is also known as Android Marshmallow. We used the unmodified version of the operating system, as provided by Google, in order to eliminate any problems due to modifications of the OS by e.g. third-party smartphone manufacturers.

Besides the review, which covers the user experience of the apps, comprehensive tests on malware protection rates and battery consumption are provided. Additionally, a short table showing any anti-theft functions included in the product is included at the end of each product report.

Many of the products reviewed and tested have components which are not security-related. The review will focus on the security features – anti-malware, anti-theft and privacy – and only mention any other functionality briefly. The structure of each product report is identical, allowing readers to compare products easily.

The main purpose of a mobile security product is to protect users and their devices from potential harm inflicted by malicious apps. Readers should note that recent Android versions incorporate some basic anti-malware features. Google's *Safe Browsing* API checks apps on installation, and protects against malware and phishing links when the user is surfing the Internet with the Chrome browser.

Additionally, an anti-theft component in a security app could be used to retrieve a lost or stolen phone, and/or prevent access to any personal data stored on the device. Basic anti-theft features (lock, locate, wipe and alarm) are provided by recent versions of Android itself.

More details of the security measures in Android Marshmallow are provided in the next section. Amongst other things, this report aims to help readers decide whether they would benefit from the more comprehensive and sophisticated security features provided by a third-party security app.

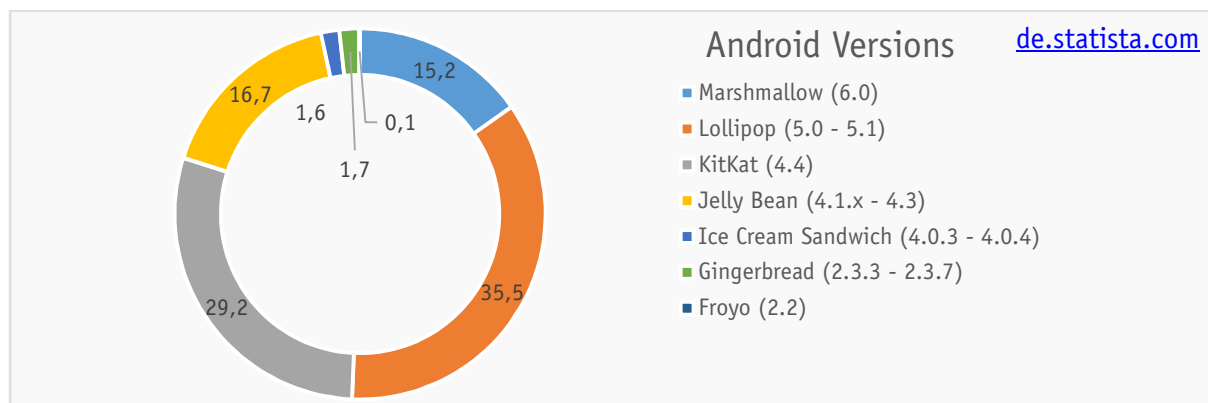
On the following pages we provide a brief overview of the risks facing smartphone users from malware and the loss or theft of their device, and discuss the benefits of security apps. We start by introducing Android Marshmallow and its new permissions system, and mention the restrictions in the operating system that security vendors have to deal with. After that we give a short summary of commonly implemented security features and their main sub-components.

At the end of the introduction we summarise the participating security products and present the results of the Malware and Battery Drain tests. Detailed reviews of the individual products follow, in which we will shed light on the layout and usage of the features.

Android Marshmallow

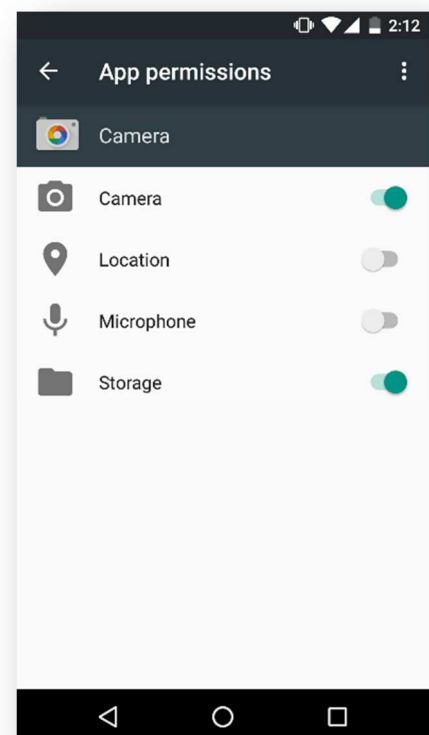


Shortly after our last Mobile Review came out in September 2015, Android version 6.0 (also known as Android Marshmallow) was released. As shown in the graph below¹, it currently holds a market share of around 15 percent. The relatively slow spread of the new version might be related to the fact that only a few manufacturers provide operating-system updates for older phones, whilst many distribute the latest Android version on only brand-new phones. We decided to use Android 6.0.1 for this review, as it was the most recent version that was available to test at the time. Android 7.0 was only released after the editorial deadline.



The new permission-management system in Android 6 introduces individual post-installation, run-time permission requests. An app designed for the new system will ask for a specific permission the first time it needs it. This gives the user the opportunity to grant an app only the specific permissions which he/she wants it to have. Apps which are designed for an older version of Android will still ask for all-or-nothing permissions on installation. Even though it may be possible to remove some individual permissions from an app after it has been installed, the app is not guaranteed to work properly if this is done, and might just fail completely when attempting to perform an action for which permissions have not been granted.

As seen in the screenshot on the right, single permissions for an individual app can be manually granted or revoked from within the Android app settings. Obviously revoking the Camera permission from the Camera app will make the app useless. But if the user were to do so, a well-implemented app would simply request this specific permission the next time it was used.



¹ <https://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/>

Additionally, a small but relevant change for security apps was introduced with the new API level 23, related to the account management. With the new API, apps can't remove accounts (such as the main Google account) from the phone. Only accounts which were created by the app itself can be removed. Obviously such limitations can be regarded as enhancing the security of Android, as such potentially destructive operations are denied by the system, but with previous Android versions this feature was used to perform a data-only wipe by many security products. Such a wipe has the advantage that all sensitive data can be removed from the phone without losing the ability to control the anti-theft features provided by the installed security app. Without removing associated accounts from the phone, emails and the Google Play Store might still be accessible.

It should be noted that all of this relates to a rather a theoretical problem. As mentioned in previous reports, if a phone has been encrypted and set up properly with a lock screen, it is virtually impossible for a thief to retrieve any data from it.

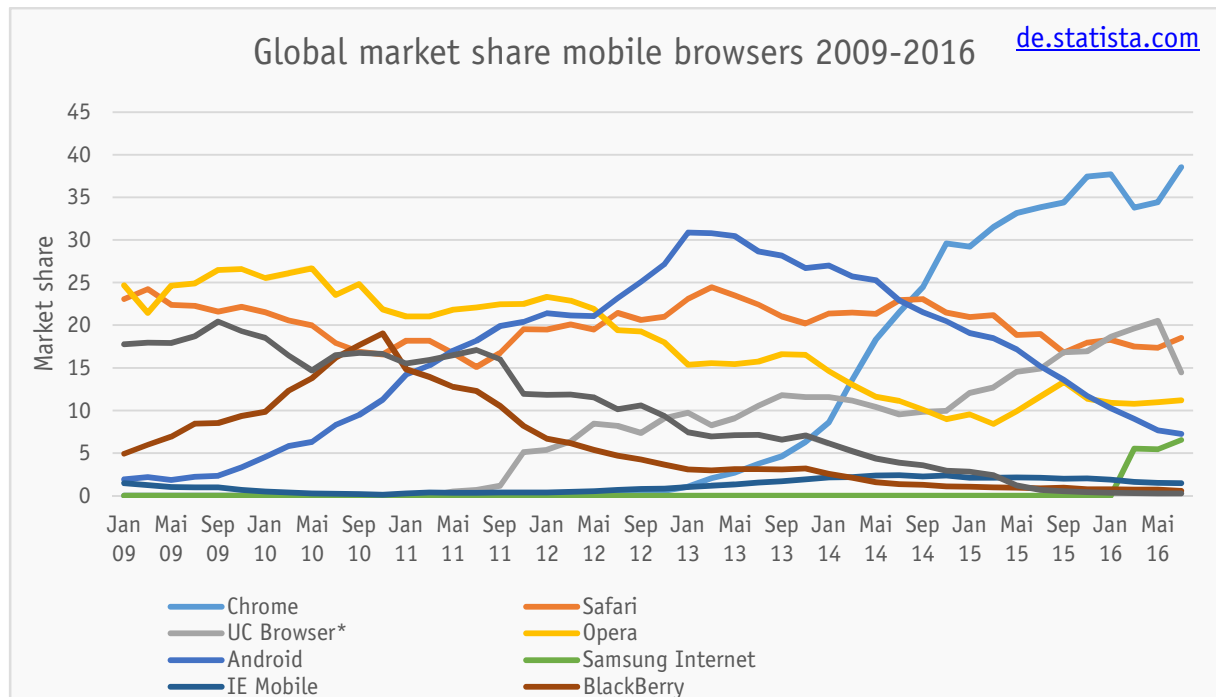
Security Features

In this section we give a short overview and discussion of common security-related components found in security products for Google Android.

The most obvious component of a mobile security app is the malware scanner. It protects the user against the inadvertent installation of malicious apps on his/her device. Similarly to antivirus programs for Microsoft Windows, mobile security apps for Android use a number of different protection components. An important feature is the real-time scanner which checks new apps during the setup process. This prevents the device being compromised by the installation of a malicious program. On-demand scanners scan the whole device for any malicious applications that are already installed, or downloaded .APK files that have not yet been run. These might be found on the device's internal storage or an external SD card. As with Windows desktop security applications, keeping malware definitions up to date is a critical factor in effective protection. Some vendors offer more frequent updates with their paid "Pro" versions than with the corresponding free versions. We noticed that many of the tested products offer a cloud-assisted malware scanner to ensure the app has access to the very latest definitions.

A privacy advisor is included in many of the tested products. It also scans the installed apps, not for malicious behaviour but for possible privacy violations. This means that apps are analyzed for uncommon, unnecessary or inappropriate app permissions, such as access to contacts, GPS position or the Internet, which could lead to the user's private sphere being breached. Some security products advise the user to uninstall any apps that are found to have given themselves such inappropriate permissions.

Some security products offer browser protection. This protects the user while surfing the Internet, by preventing the user from inadvertently downloading malicious apps, or accessing phishing websites. Some security apps offer support for a variety of different browsers, including those made by third-party app developers. In our opinion this is an important question, as many smartphone users like to use their preferred browser on their smartphone. We noticed that some of the tested products only offer support for the standard Android browser. In our opinion this is inadequate, as the stock browser was removed from Android version 4.4 and there has not been a standard Android browser in the OS versions that have appeared since then. The graph below shows the market share of mobile browsers as at July 2016. The Android browser only has a share of 7.27%, with a decreasing trend. Please note that Android 4.4, the first version not to have a standard browser integrated, first became available at the end of October 2013.











































A major component in various security apps is the anti-theft module. It is designed to execute commands on a device that has been lost or stolen. As mentioned in previous sections, Android 6 includes core anti-theft features, such as remote locking, location, wipe and an alarm sound. Many of the security products we tested extend this base functionality with additional features such as taking pictures of the thief, location tracking or automatic notification in the event of a SIM-card change. The anti-theft components are controlled via a web interface or text-message commands. The latter have the advantage that they work even if no internet connection is available, but they are less convenient to use. If the Android OS is not appropriately configured by the user, text messages are shown on the lock screen as notifications, and so texts containing e.g. the unlock code could be read by a thief. With Android 4.4 and later, app developers are no longer able to programmatically delete text messages as they arrive, and so cannot prevent the text messages used for their commands being seen on the screen when they arrive.

Some manufactures get around this issue by providing a binary SMS function, which does not show messages on the screen, in order to prevent this issue. This binary SMS system is generated by the anti-theft app itself, meaning the same app has to be installed on the friend's/relative's phone used to send the commands for the anti-theft functions.







Products tested

The products included in this year's test and review are listed below. The latest products² were taken from major app stores like Google Play at the time of the test (July 2016). After the product review, manufacturers had the opportunity to fix any flaws we found. Any problems that have already been solved are noted in the report.

Vendor	Product Name	Version	Features
 Alibaba	Ali Money Shield	5.0.1	     
 Antiy	AVL for Android	4.6	     
 Avast	Mobile Security & Antivirus	5.2.0	     
 AVG	AVG Antivirus Pro	5.4.1	     
 Avira	Avira Antivirus Security	4.5	     
 Baidu	Baidu Mobile Guard	8.3.0	     
 Bitdefender	Mobile Security & Antivirus	3.0	     
 ESET	Mobile Security & Antivirus	3.3	     
 G Data	G DATA Internet Security	25.10	     
 Kaspersky Lab	Kaspersky Internet Security	11.11	     
 McAfee	McAfee Mobile Security	4.6	     
 Tencent	WeSecure	1.4	     
 Trend Micro	Mobile Security & Antivirus	8.0	     

Symbols

To give you an easy overview on the features of a product we are introducing symbols like we are already using on our website. At the beginning of every report you will find all these symbols either orange which means the product includes such a feature or greyed out if it doesn't.

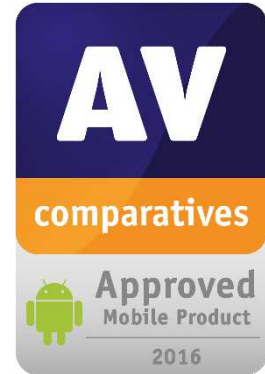
Anti-Malware		includes a feature to scan against malicious apps
Anti-Theft		includes remote features in case the smartphone gets lost or stolen
Safe-Browsing		includes a web filtering feature to block dangerous sites
App Audit		includes features to audit installed apps
Anti-Spam		includes features to block unwanted calls and/or SMS
Backup		includes a feature to backup files on the smartphone

² A comprehensive overview of the mobile security products available on the market can be seen on our website: <http://www.av-comparatives.org/list-mobile/>

Overview

The perfect mobile-security product does not yet exist. As with Windows products, we recommend drawing up a short list after reading about the advantages and disadvantages of each product in our review. A free trial version of each candidate product can then be installed and tested for a few days; this should make the decision easier. Especially with Android security products, new versions with improvements and new functions are constantly being released.

By participating in this test, the manufacturers have shown their commitment to providing customers with quality security software. As this report shows, we have found some degree of malfunction in some of the tested products. The manufacturers of the affected products have taken these problems seriously and are already working on solutions. As the core functions of all the products we tested reached a very good level, we are happy to present our "Approved Award" to all participating manufacturers.



Alibaba Ali Money Shield is an easy-to-use product, clearly focused on security and payment protection.

Antiy AVL for Android accomplishes the basic tasks of an Antivirus app effectively, namely scanning for malicious apps.

Avast Mobile Security & Antivirus provides well-implemented features for almost any use case.

AVG Antivirus Pro provides a feature-rich security app which in the free version also fulfils the basic task of malware and theft protection.

Avira Antivirus Security provides a well-designed app which provides effective protection against malware and theft.

Baidu Mobile Guard is an easy-to-use product with important security features like Wi-Fi check and an AV scanner.

Bitdefender Mobile Security and Antivirus provides an easy-to-use product which offers great protection against malware as well as anti-theft.

ESET Mobile Security & Antivirus is a well-developed security application for Android that concentrates on its core features.

G Data Internet Security is a comprehensive mobile security application that offers lots of functionality to premium subscribers.

Kaspersky Internet Security for Android is an easy-to-use mobile security app for users who want to install a single application and have done with it.

McAfee Mobile Security provides a great security product with good malware detection and a comprehensive anti-theft component.

Tencent WeSecure represents a basic, lightweight anti-virus application.

Trend Micro Mobile Security for Android is a comprehensive app that provides an advanced security concept.

Protection against Android malware

Methods of attacking mobile devices are getting more and more sophisticated. Fraudulent applications attempt to steal users' data or money. To reduce the risk of this happening, follow the advice given here. Only download apps from Google Play or reputable app makers' own stores. Avoid third-party stores and sideloading³. Another indication of untrustworthy apps is irrelevant access rights. For example, an app that measures the speed at which you are travelling has no need to access your phone book or call log. Of course, even if an app does this, it is not a clear-cut indication that it is malicious, but it makes sense to consider whether it is genuine and should be used. A look at the reviews in the app store is also a guide; avoid apps with bad or dubious reviews. If you Root your smartphone, you will have more functionality on the phone, but equally the opportunity for malicious apps to take control will also increase. Another point to consider is the warranty. It is not legally clear-cut whether the warranty is still valid if the phone is rooted. In many cases, the warranty will be considered null and void.

How high is the risk of malware infection with an Android mobile phone?

This question is difficult to answer, as it depends on many different factors. In western countries, if using only official stores such as Google Play, the risk is much lower than in many Asian countries, especially China. Many rooted phones and unofficial app stores can be found there, increasing the chance of installing a dangerous app. In many parts of Asia, the smartphone is used as a replacement for the PC, and is frequently employed for online banking. Banking apps are also becoming more popular in Europe and the USA. There is a high risk involved in receiving the TAN code on the same phone that is used to carry out the subsequent money transfer. In western countries, assuming you stick to official app stores and don't root your phone, the risk is currently relatively low, in our opinion. However, we must point out that "low risk" is not the same as "no risk". In addition, the threat situation can change quickly and dramatically. It is better to be ready for this, and to install security software on your smartphone. Currently, we would say that protection against data loss in the event of the phone being lost or stolen is more important than malware protection.

AVC UnDroid Analyser

At this point, we would like to introduce AVC UnDroid, our new malware analysis tool, which is available free to users. It is a static analysis system for detecting suspected Android malware and adware and providing statistics about it. Users can upload .apk files and see the results in various analysis mechanisms.

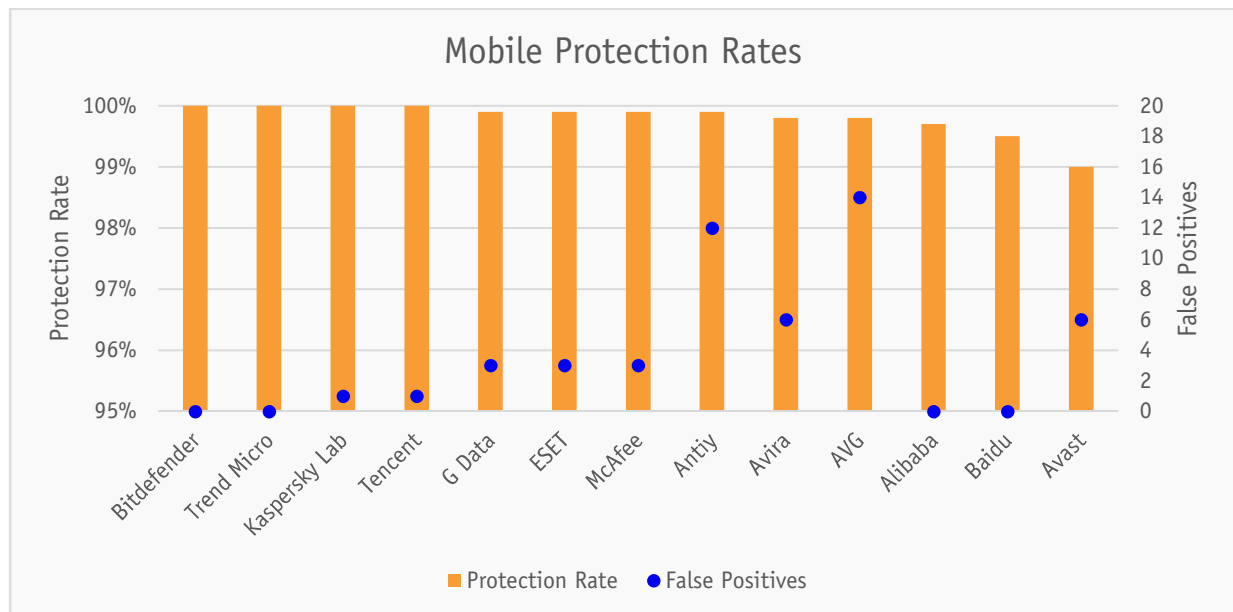


We invite readers to try it out: <http://www.av-comparatives.org/avc-analyzer>

³ <http://en.wikipedia.org/wiki/Sideloadng>

Test Set & Test Results

The malware used in the test was collected by us in the last few weeks before the test. We used **3,729** malicious applications, to create a representative test set. So-called "potentially unwanted applications" were not included. The security products were updated and tested on the 12th July 2016. The test was conducted with an active Internet connection on genuine Android smartphones (no emulators were used). The test set consisted exclusively of .APK files. An on-demand scan was conducted first. After this, every undetected app was installed and launched. We did this to allow the products to detect the malware using real-time protection. A false-positives test was also carried out. The results can be seen below (sorted by Malware Protection and number of False Alarms).



As can be seen above, the protection rates against real Android malware are very high. This might be due to the increasingly aggressive detection by app reputation for apps that are not on Google Play, but also because many of the participants in our test are leading mobile security vendors with good protection rates.

Mobile Protection Rates		
	Protection Rate	False Positives
Bitdefender, Trend Micro	100,0%	0
Kaspersky Lab, Tencent	100,0%	1
G Data, ESET, McAfee	99,9%	3
Avira	99,8%	6
Antiy	99,8%	12
AVG	99,8%	14
Alibaba	99,7%	0
Baidu	99,5%	0
Avast ⁴	99,0%	6

⁴ Avast has an option to report/detect apps which are not very widespread and are deemed as suspicious. With this option, Avast would score 99.9% and have 37 FPs. Avast noted that that FPs would not be encountered if apps were installed from well-known and reputable stores which they have whitelisted.

Battery Drain Results

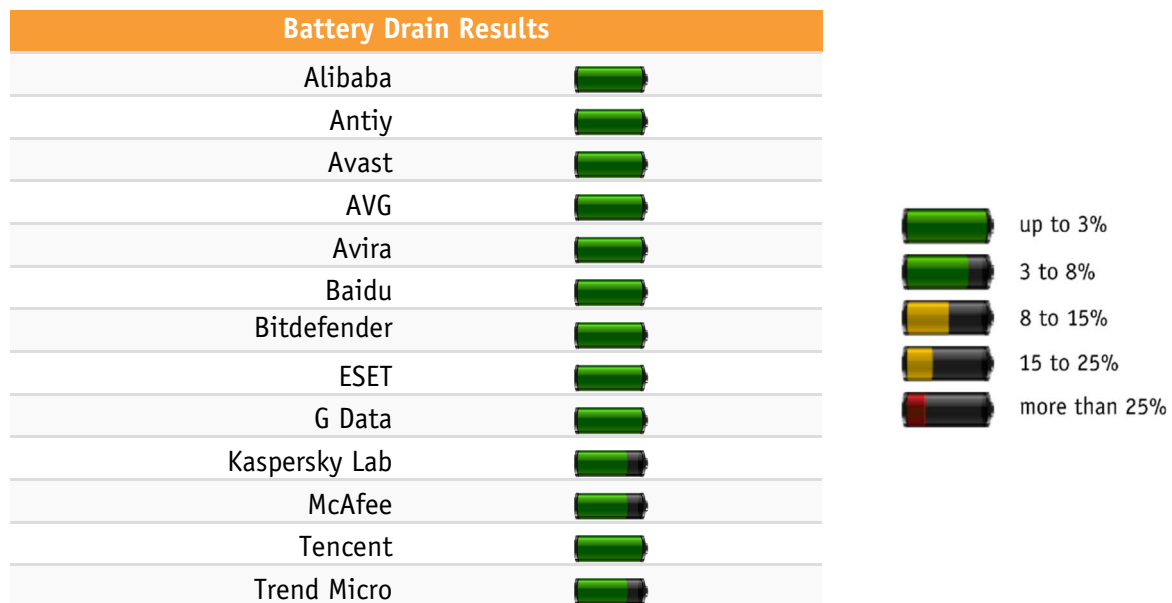
As in our previous reports we measured the additional power consumption of an installed mobile security product.

Testing the battery usage of a device might appear at first glance to be very straightforward. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones, the usage patterns of different users are very varied. Some use the multimedia functions extensively, others view a lot of documents, while some use only the telephone functions. We need to differentiate between power users, who take advantage of all of the possible functions in the device, and traditional users who merely make and receive phone calls.

The test determined the effect of the security software on battery use for the average user. The following daily usage scenario was simulated:

- 30 minutes telephony
- 82 minutes looking at photos
- 45 minutes surfing the Internet with the Android browser
- 17 minutes watching YouTube videos with the YouTube app
- 13 minute watching videos saved on the phone itself
- 2 minutes sending and receiving mails with the Google Mail Client
- 1 minute opening locally saved documents

In our test, we found that most mobile security products have only a minor influence on battery life.



In general, we were able to give the tested security suites high marks. Three products in this year's test showed a slightly increased battery drain: **Kaspersky Lab**, **McAfee** and **Trend Micro**.



Alibaba

Ali Money Shield

5.0.1



Introduction

The Ali Money Shield is a free security product, which includes performance and various security components, but clearly focuses on providing protection for users with a Taobao.com account.



Usage

In the initial setup the “Ali Installation license and service agreement” is already marked as accepted. After the user taps “Enter Money Shield 5.0”, the user is directed to the main program window. After each start, Ali Money Shield automatically performs a quick security check of the device.

AV Scanner

The AV Scanner is part of the Tool Box and by default, performs a quick scan. In the scan settings, the user can change the default scan action to full system scan, and update the virus definitions manually.

Theft protection

Only users with a Taobao account can use the Ali theft protection feature. The Ali app requests administrator permissions for the device. Via the web interface qd.alibaba.com, the smartphone owner can sound an alert on a misplaced device, locate it, or wipe personal data.

In our test, the app successfully deleted all contacts, the call log and all pictures. Nevertheless, text messages were not deleted as described, even after repeated attempts to explicitly erase them. With the device’s front-facing camera, the app successfully snapped two pictures of the “thief”, and displayed these within the web interface.

Quick check-up

The quick check-up rates the phone’s security status according to Alibaba’s scoring rules. The result of the checkup is displayed on the main program tab of the “Ali Money Shield”. Users can earn additional health points by activating their Taobao protection, conducting a deep AV scan, and protecting themselves against privacy and security risks from applications. On the same tab we can see how many calls and nuisance text messages have been processed by the Ali app.

Tool Box

Besides a file and memory clean-up, the tool box provides the *AV-Scanner*, *Payment Guard*, an app lock, a fraud blocker and a Wi-Fi scanner. Additionally, the Ali theft protection can be found here, which requires a *Taobao* account.

On the final tab, we find a feature to uninstall applications, access the the Ali app store, and Ali 110 to report to Taobao-related problems such as hacked Taobao accounts.

Fraud and Nuisance Blocker

Unsolicited sales calls are an irritating and annoying interruption all Chinese smartphone users have to cope with. In our test, the app correctly marked mobile and landline phone numbers that at the time of the review had been used for unsolicited sales calls.

My Safebox

Here users can add their Taobao account numbers and identify themselves as the rightful owner of the account. For authentication, a text message is sent to the mobile phone number that is registered with the Taobao account.

Task bar

Via the Ali taskbar we have easy access to smartphone tuning, a “safe” OCR scanner, clean-up functions and a flashlight. Furthermore, the number of nuisance calls/text messages that have been intercepted by the Ali app is displayed.

The Ali spaceship

After installation of the Ali app, our test device had a tiny circular object (“spaceship”) on one side of the mobile desktop. After the user drags this spaceship to middle of the screen, the application performs a quick clean-up.

Conclusion

Ali Money Shield is an easy-to-use product, clearly focused on security and payment protection. We very much liked the simple design, which is not overloaded with features.

However, we recommend adding a deinstallation password to the theft-protection functionality.

Anti-Theft Details		
Commands Web		
Alert	✓	
Lock	✓	
Wipe	✓	
Additional Features		
Face Cam	✓	Takes a photo of a potential thief



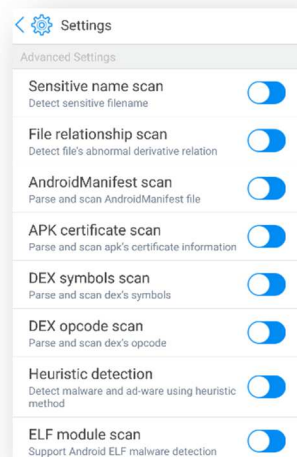
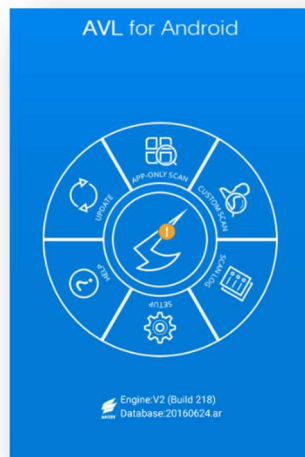
Antiy

AVL for Android
4.6



Introduction

AVL for Android is a security app that concentrates on malware-scanning features. This is also implied by their slogan *We focus on Antivirus Engine*. Additionally, safe browsing and call-blocking features are provided, please see details of these below.



Usage

After installation, the app opens directly on the home screen, no initial setup or acceptance of terms and conditions is needed.

Anti-Virus

The app provides both custom and app-only scans, which can be run manually. With the former, options to scan the installed apps on the mobile phone or the APK files on the SD-Card are provided. Additionally, real-time scans are run on any new apps when they are installed. Scans already performed can be viewed in the scan log, in which individual results for each scanned file are listed.

Scan options, like the usage of heuristics, can be adjusted in the settings. The settings are found under the menu button "Setup". In *Settings*, you can open or close any different scan options depending on your own needs. AVL for Android can output the fine-grained scan reports about the malicious or suspicious

apps for your reference, and provides a one-click clean-up function to remove all the malicious apps detected. In addition to configuration options related to the scans, the safe browsing and call-blocking features can be found here. When we tested the safe browsing feature, none of the tested malicious sites were blocked. We note that the call-blocking feature only worked with Chinese telephone numbers in our test.

Conclusion

AVL for Android accomplishes the basic tasks of an Antivirus app effectively, namely scanning for malicious apps. It also provides abundant configuration options, which allow the user to fine-tune the scan.

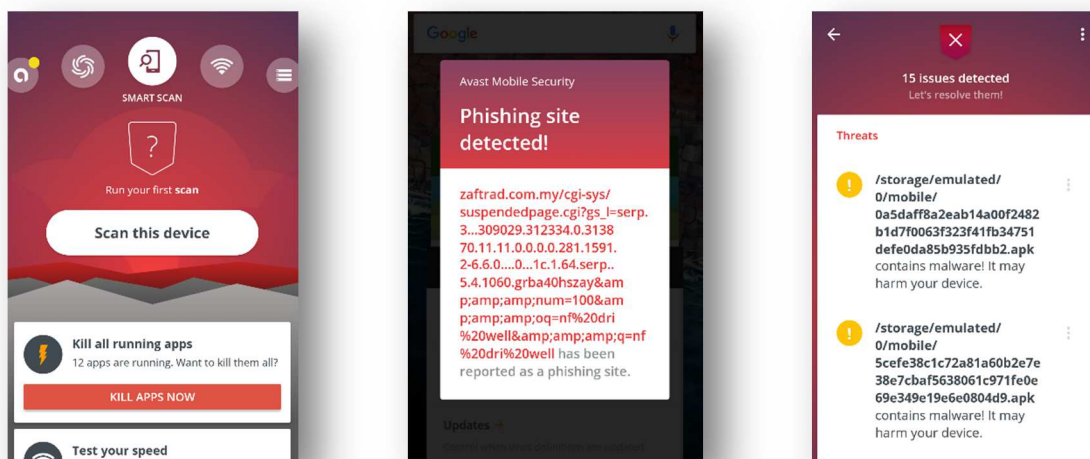
For users whose major concern is file scanning, this app would easily be sufficient.



Introduction

Avast is a comprehensive product which has always offered a great range of security features. The version tested this year has brought some major changes and a completely new design. This also can be seen in the version number; in our Mobile Test of 2015 we tested version 3.0, while this year we already had version 5.2.0. Due to the many features available, Avast has made non-essential functions into separate apps, so users can decide which features they want to install and use. Therefore, besides the anti-theft feature (which because of security reasons has always been a separate app), the following apps are provided by Avast but not covered by our test: *Cleanup*, *Battery Saver*, *SecureLine* (VPN Service), *Passwords* (Password Manager), *WiFi Finder*

The main app provides the anti-virus function, app locking, call blocking, a privacy advisor, a Wi-Fi-speed and security check, as well as a firewall. The latter is only relevant for users who have rooted their phones.



Usage

After the installation, the EULA has to be accepted, then the user is directed to the home screen where a first scan is suggested.

Smart Scan

The main feature of the app is the smart scan. Avast has abandoned complicated customisations, and provides an easy one-click experience. In the settings we only find options to toggle the detection of PUA/PUP, and warnings for apps with a poor reputation. A scheduled scan can also be set.

A scan is responsible not only for file scanning but also for checking for other potential risks such as installation from unknown sources or USB debugging being enabled. Advanced users who have deliberately enabled such insecure features can suppress their warnings easily.

Anti-Theft

This feature comes as a separate app, which can be controlled by text message or web interface. The initial configuration sets up a PIN code which locks the app and also is used for SMS commands. Additionally, an account is created which can be used to control the app via the web control. To use commands like the “audio record” the app has to be connected to *Google Drive* to store the data. To hide the app from a potential thief stealth mode can be activated which hides the app shortcut in the menu. The web commands are easy to use, with a well-designed interface. As noted in the Anti-Theft details section, for recording audio and photos, the app needs to be linked with Google Drive so it can upload the created files. Unfortunately, there is no prompt for this in the setup process of Anti-Theft, and therefore it can easily be missed. If text-messages are used to send anti-theft commands from e.g. a friend’s phone, these ideally be sent from another phone with the Avast app, as these will not be shown anywhere. Avast inform us that standard text messages can be used as well, although we had difficulty finding this function.

Wi-Fi Check

This tool checks available Wi-Fi networks for threats and establishes if it is safe to use them. This is done by checking things like the encryption used. After such a test has been run, it is also possible to check the connection speed.

Call Blocking

The call blocking feature is implemented as a simple “blacklist” but when using the rule “All unknown numbers” it is effectively whitelisting known numbers. In our test this feature worked as expected, and managed to suppress an incoming call. On our test system, the phone rang once before the call was blocked; Avast inform us that this only happens with some (older) mobile phones.

App Locking

It is easy to protect apps from unauthorized usage with a PIN code. The protection works fine, and Avast shows a lock screen every time a protected app is used. In our test, we could not uninstall the Avast app via the Android settings, but we were able to remove it by dragging its icon on the home screen, which obviously removes all its protection features.

Privacy Advisor

The privacy advisor lists installed apps and shows the permissions each one has, as well as ad networks used.

Conclusion

Avast provides well-implemented features for almost any use case. Its well-designed Smart Scan and the additional Anti-Theft App provide a great user experience for these core features. Uninstall protection for the App-Lock app itself, and accepting standard text messages for anti-theft functions, would be useful improvements.

Anti-Theft Details		
Commands Web		
Locate / Track	✓	Displayed on <i>Google Maps</i> Map
Mark as Lost	✓	Triggers configured actions like tracking, lock, siren, ...
Forwarding	✓	Allows to forward all incoming calls and SMS to a given number.
Siren	✓	
Lock	✓	
Wipe	✓	
Launch Anti-Theft	✓	Opens Anti-Theft user interface on device
Record Audio	✓	Records audio for a predefined duration of 1-5 minutes, needs enabled Google Drive
Take Picture	✓	Takes a picture with the front or back camera. Optional: The camera is triggered when the screen is turned on. Needs enabled Google Drive
Get data	✓	Allows to fetch data (calls, SMS, contacts) from the device. We found it quite hard to find the fetched data.
Initiate Call	✓	Allows to call a given (in web interface) phone number
Show Message	✓	Allows to send a single message, which is shown as popup
Commands SMS		
Message	✓	As already mentioned SMS commands are set from within the Avast app. This
Mark as Lost/Found	✓	enables the usage of binary SMS which can't be read on the receiving phone.
Lock	✓	To get SMS answers from the receiving phone SMS responses have to be explicitly activated. In our test all commands worked as expected only the
Siren	✓	locate command works in an unexpected way. The behaviour of the locate
Locate	✓	command is strange, the evaluated location will not be sent back to the
Call	✓	phone who triggered the call but rather sent it to a set "friends" number
Forward	✓	which can be set in the advanced settings.
Wipe	✓	
Additional Features		
SIM Change Protection	✓	Sets the phone status too lost



AVG

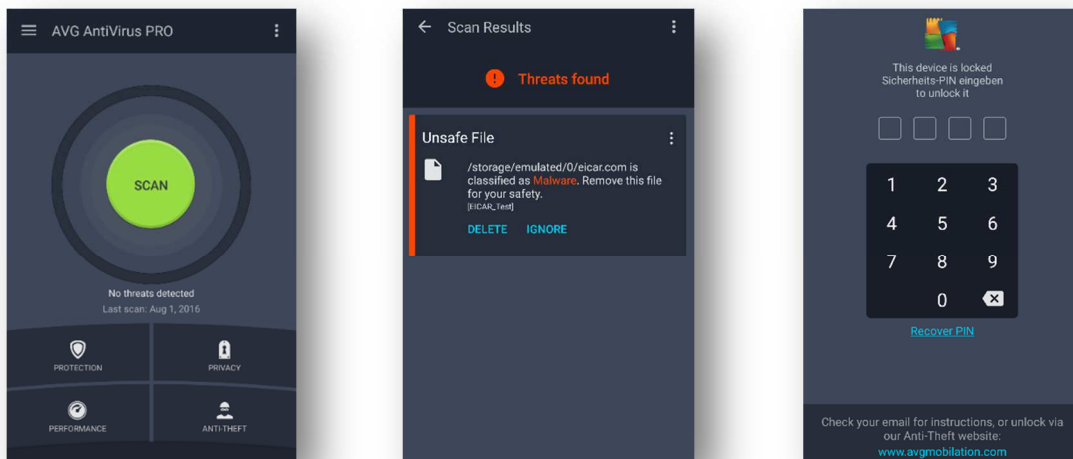
AVG Antivirus PRO

5.4.1



Introduction

AVG provides a comprehensive app with a clear and easy to use design. It comes in a free and a Pro version, whereby the Pro version enables “Camera Trap”, “Device Lock” (on sim replace), “App Lock” and “App Backup”. Additionally, advertisements are removed in the Pro version.



Usage

The app starts up to a clean home screen from where the main components of the app can be reached. A green circle shows that everything is in order, and no threats have been detected. On the first start this circle flashes up orange, which indicates that a first scan should be started. A scan can be started by pressing this circle. In the event of a threat, the circle changes its colour accordingly. A red circle indicates unsafe files like malware found, and an orange one unsafe settings like an enabled debug mode.

Antivirus

As mentioned above, a simple scan can be started directly from the home screen. If threats have been found, we can see the scan logs by pressing on the button again. In the protection menu we can find the settings for the scan, a file scanner and a list with ignored threats. A manual update can also be triggered from here.

In the scan settings we can also find the Safe Web Surfing component which protects us from threats like phishing. However, in our test we couldn't provoke even a single detection using *Google Chrome*. As mentioned in our introduction, this is unacceptable, considering the default Android browser was removed from Android in version 4.4 (KitKat) which was released in late 2013.

Anti-Theft

The Anti-Theft component can be handled via a decent web interface or text message. In our test, all the commands worked as expected. To perform a factory reset when wiping the phone, the app has to be made a device administrator. If this has not been done, AVG tries to delete data without a factory reset. In our test, only files on the internal storage and the call log where deleted. Data like the text-message Logs, Browser History and our logged in Accounts were not wiped.

Privacy

This component offers app locking, call blocking and an app backup, which simply saves the Android installation files to the SD card. Additionally, it offers Wipe by Category, which lets you wipe your contacts and/or call logs. These components seem to work conveniently, with exception of the call blocker which lacks usability and blocking options.

Performance

This component provides tools to monitor data, storage and battery usage and provides some optimisations for these.

App Lock

Here one has the possibility to protect sensitive apps with a password. AVG helps by suggesting sensitive apps which should be locked.

Vault

This provides an encrypted space to store photos.

Battery Usage

This component monitors the battery usage of the phone. It is possible to set a battery level at which the user should be warned, as well as one where the phone should go in power-saving mode. This mode will disable features like Bluetooth and Wi-Fi to save battery.

Task Killer

Task Killer shows all currently running apps. It is possible to kill each of them separately or all at once.

Conclusion

AVG provides a feature-rich security app which in the free version also fulfils the basic task of malware and theft protection. The Pro version impressed us with additional security features like the device lock on SIM replacement.

Anti-Theft Details		
Commands Web		
Shout	✓	Plays the devices ringtone, which can be stopped on the phone
Locate	✓	Displayed on <i>Google Maps</i> Map
Lock	✓	Locks device with a definable 4-digit PIN, a custom message can be displayed
Unlock	✓	Unlocks a phone locked by AVG
Wipe	—	
Security PIN	✓	Changes the PIN which is used for SMS commands and to lock your device
Commands SMS		
Shout	✓	
Locate	✓	
Lock	✓	If SMS are used because there is not internet connection available on the phone, pressing the "Forgot Password" option butts the lock screen in bugged state
Wipe	—	
Additional Features		
Camera Trap	✓	
SIM Protection	✓	Locks your phone if the SIM is replaced


Avira

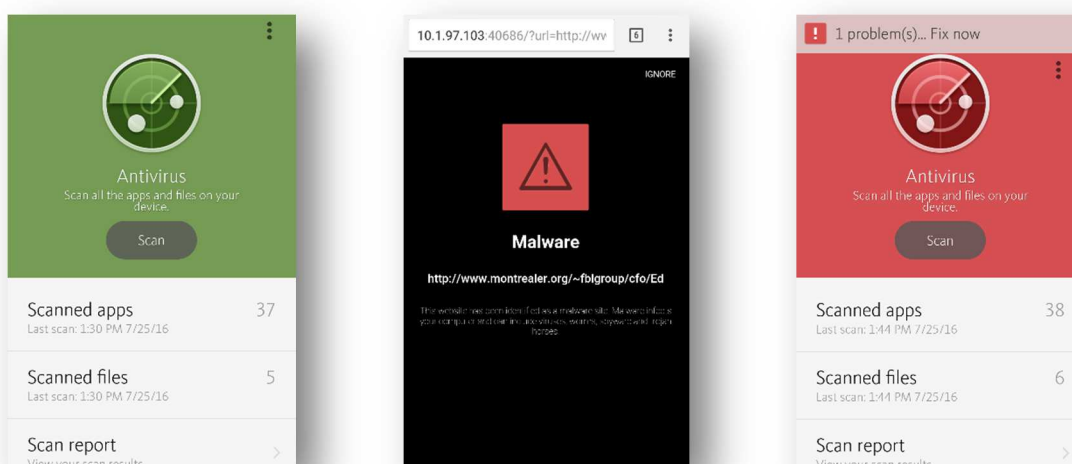
Avira Antivirus Security

4.5



Introduction

Avira provides a comprehensive product which is available in a free and a Pro version. The core features of Avira are the malware protection as well as the Anti-Theft component. Additionally, *Avira SafeSearch*, *Identity Safeguard*, a blacklist for unwanted calls and a Privacy Advisor are provided. The Pro version enables Secure Browsing as well as more frequent antivirus database updates. Avira Optimizer and App Lock are offered as separate apps.



Usage

On the first start, one is guided through a welcome tour, which introduces the components of the app. After that we are prompted to register or log in to the app followed by an initial malware scan of the phone. To login we can use either a Facebook or Google Account or create an own Avira account.

Antivirus

The Antivirus component offers a one-click experience, whereby advanced users can configure the scan in the settings. It is possible to optionally scan for adware, PUAs and riskware, and choose if apps and/or files should be scanned. Additionally, a scan can be triggered whenever storage is mounted or a USB cable is unplugged. A scan scheduler is also offered which lets you set automatic scans at specific times.

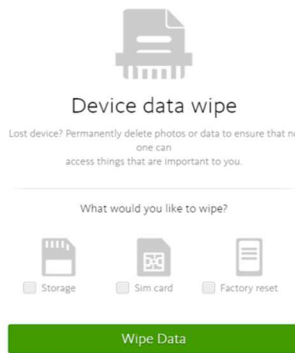
In the Pro version the user is additionally protected with secure browsing, which warns of harmful sites such as malware and phishing pages.

The virus database is updated automatically whereby Pro users get them more frequently.

Anti-Theft

The Anti-Theft component offers web control but no text-message control. The commands all worked as expected and we were not able to bypass the Avira lock screen.

The Wipe function offers the three options Storage, SIM Card and Factory Reset as shown in the following picture:



Storage and Factory Rest worked as expected but we were able to restore the data on the SD card with a common recovery tool. In our tests we were not able to delete data stored on the SIM card. To be fair, it has to be mentioned that it is not that easy to write to a SIM card in the first place. Recent Android versions simply don't offer the option to store contacts or SMS on the SIM card anymore. Therefore, deleting SIM cards is not a big issue nowadays.

Additional Features

In addition to the core features, Avira provides a Blacklist to block unwanted calls, "Avira

SafeSearch" (a widget that enables searching via Avira's own search engine), "Identity Safeguard", which looks up databases of email addresses known to be compromised, and "Privacy Advisor", which rates the privacy risk of apps according to their permissions.

In addition to those features directly integrated into the app, two separate apps offered by Avira, namely "App Lock" and "Avira Optimizer", can be installed. The first provides password protection for apps, while the later tries to optimize your phone's storage and battery.

Conclusion

Avira provides a well-designed app which provides effective protection against malware and theft. The latter relies on web commands, and we feel additional text-message commands would be a nice addition. The execution of the Wipe command is a bit confusing, and users who are not willing to experiment with the different options might not get the expected results.

Anti-Theft Details		
Commands Web		
Locating	✓	Displayed on <i>Google Maps</i> Map
Play Sound	✓	Plays a sound for 20 seconds.
Lock Your Device	✓	The phone will be locked with a new PIN defined in the web interface. Additionally, a message and a contact number can be displayed.
Device Report	✓	Gives you available information of your Phone like IMEI and device model.
Wipe	—	SD-Card data is restorable. SIM-Card wipe not working.



Baidu

Baidu Mobile Guard
8.3.0



Introduction

Baidu Mobile Guard is a free security product, which offers many functions including mobile tuning, protection against security and privacy risks, mobile payment protection and a family guard function.



Usage

The installation process creates a *Payment Safe* icon on the home screen of the smartphone. Within the *Payment Safe* component we find the ride-sharing app *Didi Chuxing*, which is installed on our test device, marked as already protected. After the user taps "Enter Guard", the user is directed to the main program tab.

AV Scanner

An AV scan starts automatically, and after the scan is finished, we can access the scan settings in the result tab. Cloud scan is activated by default and all app installations are automatically checked. We can start a full scan manually and we can allow Baidu to upload unknown samples when our device is connected to Wi-Fi.

Security Protection

The current Baidu app offers a whole set of functions to protect the user from various security threats. After each tap, the app carries out an automatic security check. From within the security tab, we can scan the device for malicious apps, check the safety of our Wi-Fi, scan for system vulnerabilities and test the safety of the payment environment.

Frequently used functions

On this tab, Baidu offers smartphone speedup, trash cleaning, security protection, a family guardian, an app store and app management.

Initial check-up

The user sees in the center of the tab a circular display showing the current health of the mobile device. When the user taps the display, the app removes system trash, ends processes, analyses apps and activates various protection features such as text-message fraud protection, telephone fraud protection, and a test of the network environment.

Mobile Speedup and Trash Removal

After our check-up, the mobile phone speedup found no further way to speed up the system. Nevertheless, the trash removal function found 20.4 MB of system cache, leftovers from APP deinstallations and app installation packages. The Baidu Mobile Guard reported the detection of leftovers of LeTv Sports, an app that we had not installed on our test device.

Family Assistance

Baidu Mobile Guard offers an Assistance function for older, perhaps less smartphone-literate family members. To become an Assisted Person, a user has to install the Baidu Mobile Guard or accept an invitation by text-message from the Assistant to install the app. After the Assisted Person has approved the Assistant, he/she can contact him/her with a single tap on the tiny phone icon next to the Assistant's phone number. The Assistant can connect to the Assisted Person's phone and conduct remote tuning operations such as trash removal and checking for phone calls and text messages blocked by this app. The remote check of the data volume and mobile phone balance also worked in our test. Our test Assisted Person was informed by the app of our check. Locating our Assisted Person's phone also worked as expected.

Treasure Box

Users can access a variety of features via this tab. Baidu offers security and privacy-related functions such as antivirus, a disturbance blocker and a lock that controls app access with a gesture password. We also found a secure

text-message feature that asks to take over as the default text-message app on our smartphone, and permission management that needs to be installed in the form of separate app. Non-security features include a general app store and a Wi-Fi management tool. Finally, Baidu offers its users a feature to root the smartphone, and a shortcut for installing Baidu Search.

Fraud and Nuisance Blocker

Unsolicited sales calls are an annoying interruption all Chinese smartphone users have to cope with. In our test, the app correctly marked mobile and fixed-line phone numbers that at the time of the review were being used for unsolicited sales calls.

App Management

On the application management tab, Baidu provides app management functions such as deinstallation, app update and moving apps to a SD card. On the same tab, there is access to a Baidu app store and to two games.

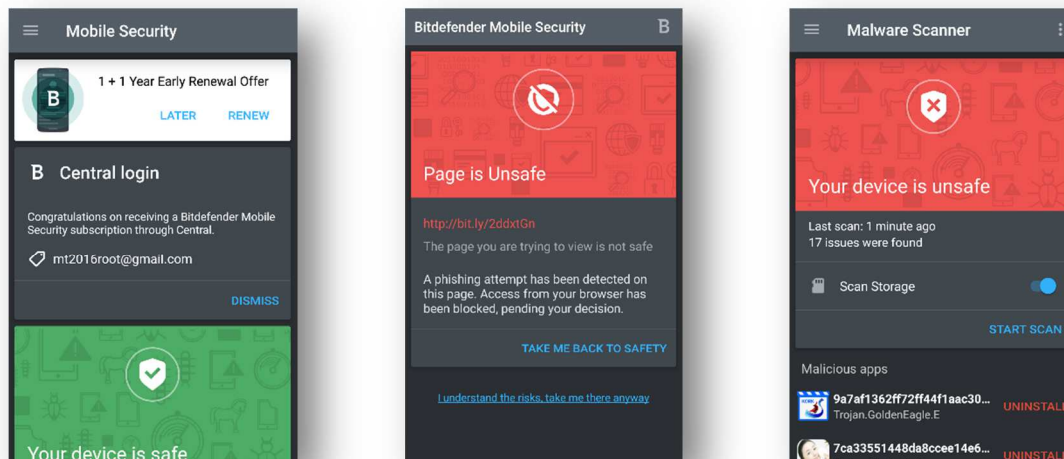
Conclusion

Baidu Mobile Guard is an easy-to-use product with important security features like Wi-Fi check and an AV scanner. The Assistance feature is new and unique. Enlarging its contact button and making it more clearly visible would further improve its usability for elderly or less smartphone-literate users. We recommend adding a full theft-protection feature, as the danger of unauthorized access to private information on stolen or mislaid mobile devices should not be underestimated.



Introduction

Bitdefender Security and Antivirus is a well-engineered paid product which can be purchased for €9.95 per year. In addition to malware protection and an anti-theft component, the app provides a privacy advisor, web protection, and an app-lock app.



Usage

During the installation process, the user has to log in with a Google or Bitdefender Account. Sending anonymous statistics is an opt-out. After accepting the EULA, a 15-day trial period starts. Bitdefender recommends running an initial malware scan.

Malware Scanner

The malware scanner checks if the device is infected with any kind of malicious software. There are not many options available. The user can only decide if the storage is scanned, and toggle the real-time protection *Autopilot* on/off. Furthermore, the *in-the-cloud detection* feature can be toggled. If it is enabled, suspect apps can be uploaded for further investigations. We liked the fact that malware scans can be triggered from the web-based control panel. This interface also displays the scan results of previous scans.

Anti-Theft

To fully activate this component, the app has to be set as a device administrator. The user has to set a 4 to 8-digit pin to prevent unauthorized access to the device. During setup, the phone number of a trusted friend, who will be notified if the SIM card is replaced, has to be entered. Furthermore, this is the one and only number which is allowed to send wipe commands via text message. The anti-theft component can be controlled using text-message commands, as well as with a well-designed control panel via the Internet.

Privacy Advisor

The privacy advisor queries Bitdefender's cloud service (which took some time in our test) to check the permissions of all installed apps on the device. Bitdefender rates the privacy in points. We got 58 points on our test device. Bitdefender gives a short introduction to the scoring, and states that lower scores are better, but does not state upper or lower boundaries

or give a hint as to what an average score would be. Bitdefender tell us that they are considering how to make this clearer. However, we liked the fact that all permissions can be viewed for each installed app. Bitdefender gives a short explanation for each permission.

Web Security

This feature protects the user while browsing the web and works with the stock Android browser, Chrome and Firefox. Bitdefender states that it protects the user from malware, phishing and other fraudulent content. Bitdefender uses its own cloud service for decision-making. In our quick test this component worked as expected.

App Lock

To use this feature, Bitdefender has to be enabled in the menu "Apps with usage access".

The component allows the user to protect installed apps with the predefined Bitdefender PIN. The function "Snap Photo" can optionally be used to take pictures with the device's front camera whenever 3 incorrect PIN entries are made. Additionally, it is possible to disable the function if the device is connected to a predefined Wi-Fi (secure environment). The component worked properly in our tests.

Conclusion

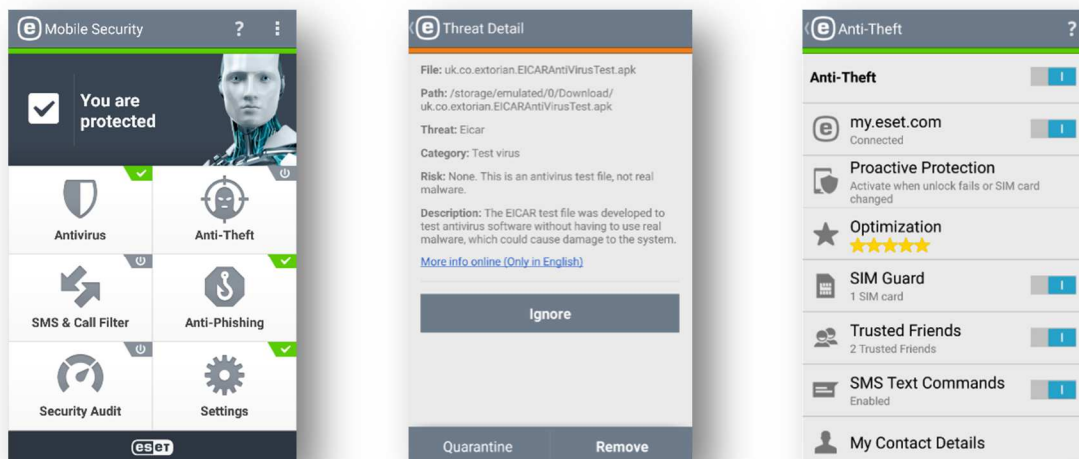
Bitdefender provides an easy-to-use product which offers great protection against malware as well as anti-theft. In our tests all features worked as expected, but please see note on lock function in the table below. As mentioned in the anti-theft details Bitdefender has to at least warn the user about the issue or provide a better solution.

Anti-Theft Details		
Commands Web		
Locate	✓	Displayed on <i>Google Maps</i> Map
Send Message	✓	Message can be displayed on screen. Optional: Alarm sound
Lock Device	✓	Locks the device with the Android lock screen. The PIN is set in the web interface
Wipe Device	✓	Factory Reset
Commands SMS		
Locate	✓	Link to <i>Google Maps</i> is sent
Lock	✗	The lock screen uses the PIN which is sent in the text message. If notifications are shown when the device is locked a thief will see the PIN in the SMS notification. Bitdefender should at least advise the user to disable notifications to prevent this issue. Bitdefender tell us that they will deal with this issue in a future update.
Wipe	✓	Factory Reset, Number allowed to wipe must start with +xx to work
Scream	✓	
Callme	✓	Call is not hidden and speaker is not muted
Help	✓	Sends the usable commands
Additional Features		
SIM change protection	✓	



Introduction

ESET Mobile Security & Antivirus is a straightforward security application for Android smartphones. At the moment, a premium license for one year costs €9.99. Among the features available *only to premium* users are anti-theft, automatic updating of the threat database, SIM Guard, SMS & call filter and scheduled scans.



Usage

On first start-up users have to accept the license agreements and select their preferred language and current country. Furthermore, users have to decide whether they want to participate in ESET Live Grid (a feature that collects data, and surveys installed applications using an online database), and if potentially unwanted applications (PUAs) should be detected. No registration is required since the application uses the Google account set up on the device. New users can try the app's premium features free for 30 days.

Antivirus

For antivirus scans, three different modes are at hand. Quick mode checks all installed applications and *.dex* (executable), *.so* (library) and *.zip* archive files on the phone's own storage only.

Smart scan additionally checks the aforementioned file types on external storages like SD cards. A third option named *Deep Scan* checks every file on both internal and external memory, and is therefore the most time consuming mode. In the event of a detection a detailed description of the threat family, and assessment of its risk level, are provided. This could allow expert users to make their own decisions if they want to. Users can also choose in the application settings the server from which the signature updates are downloaded. Besides the default server, the application offers updates from a pre-release server. Real-time protection, which automatically scans files the device interacts with, can be toggled, as can scheduled scans. It is also possible for users to decide if they want the Anti-Virus to detect potentially unwanted applications (such as adware) and potentially unsafe applications.

Anti-Theft

The application's Anti-Theft feature requires some preparation before it is ready to use. Setting a password, which is needed to access the Anti-Theft settings in the future and to unlock the phone in case of loss, is mandatory. The app also requires device admin rights to enable uninstall protection. Users can authorize their current SIM card in the app's SIM-Guard feature which automatically locks the device if an unauthorized SIM card is inserted.

ESET provides a web interface for remote control, which requires a separate user account. When connection to the web interface is enabled, the application automatically goes into a proactive protection mode. On detection of suspicious activity, such as entering an invalid unlock code multiple times, the application will lock the device, track its movement and take pictures regularly.

The application also rates the optimization level of the device when connected to the web interface and suggests improvements of device configuration that enhance Anti-Theft protection.

SMS & Call Filter

With these feature users are able to block incoming and outgoing calls using black-/whitelisting. When using Android 4.4 or higher the application notifies the user that SMS can't be blocked.

Anti-Phishing

This feature did not work in our testing environment. The app itself states that some browsers might not be supported. During our tests, none of the commonly used browsers functioned with the feature. ESET inform us that this problem is specific to Android version 6.x and they will fix it in a future update.

Security Audit

With a feature called *Security Audit*, users can monitor important device configurations within the application. The audit is split into device monitoring, which concentrates on system setting, and an application audit that shows granted app permissions.

Help

If some feature appears not to function properly, or its purpose is not clear, the user can look it up in the application's help pages. They are available via a question-mark button on the top bar of the app.

Conclusion

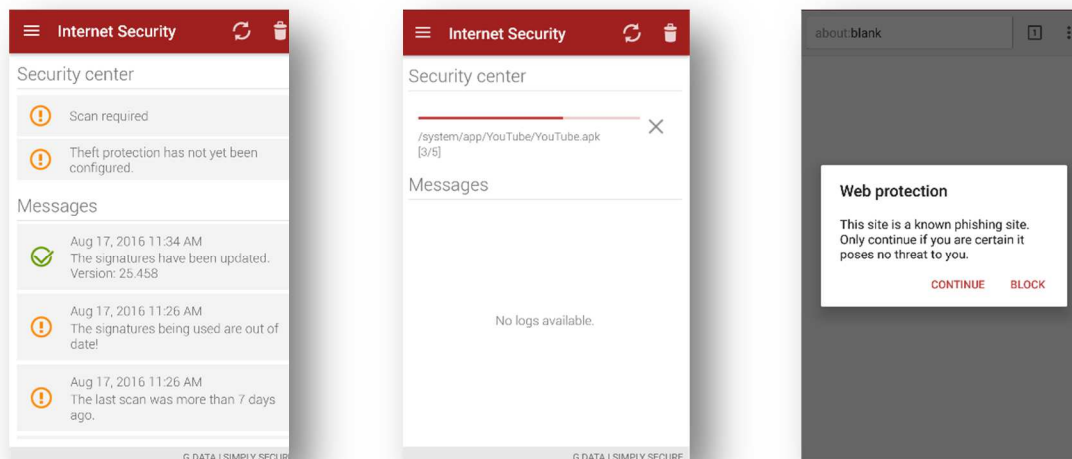
ESET Mobile Security & Antivirus is a well-developed security application for Android that concentrates on its core features. It is simply structured, easy to use and offers in-app help pages that leave few questions unanswered. Apart from the anti-phishing feature, which did not function at all, the application worked flawlessly and can be recommended to users who like to keep it simple.

Anti-Theft Details		
Commands Web		
Locate / Track	✓	Displayed on <i>Google Maps</i> Map
Mark as Lost	✓	Triggers device lock, automatically tracks phone position and takes pictures
Siren	✓	
Lock	✓	Automatically locked when marked as lost
Wipe	—	Deleted data from the SD card could easily be restored; ESET tell us this only affects some devices and they are working on a fix.
Download activity	✓	All the taken pictures and locations can be downloaded as a ZIP archive
Messages	✓	Allows user to send a single message, which is shown as pop-up
Commands SMS		
Lock	✓	
Siren	✓	
Locate	✓	
Wipe	—	As for web Wipe command
Additional Features		
SIM Guard	✓	
Uninstall protection	✓	Locks the device if device administrator rights are removed from the app



Introduction

Internet Security from G Data is an application for Android Smartphones that not only provides malware protection but also gives the user various other tools related to mobile security. Its features include theft protection, parental control, phishing protection, call filters and app management. The app is also available as a free version, though most of its features are only useable with a premium subscription.



Usage

On first start-up, Internet Security requests multiple permissions along, with a popup message explaining why they are needed. To use the app, the user has to log in or create a new account. Currently a 30-day trial period of a Pro subscription is offered to new users. In order to start the application, the user has to accept the license agreements.

Antivirus

When using the scan utilities, the user can choose to scan only installed applications or the whole system. Other app features are usable during the virus check; the current progress can be seen in the *Security Center*. The available scan settings include the option to run a scan on newly installed apps, and scheduling periodic application or full system scans in predefined intervals. The user can choose to run scans only when recharging or when using a battery-safe mode.

Anti-Theft

Before using theft protection features of G Data Internet Security the user has to set a numeric password for text-message commands in the Lost/Stolen configurations. Optionally a reference email address, to which answers to SMS commands will be sent, can be entered, as well as a telephone number from which the previously chosen password can be changed remotely. To work properly, the application also needs device-administrator rights. The users' device can be auto located when its battery runs low, which can be useful if you lose your phone when it is already short on power. Another feature of Anti-Theft is the option to sound an alarm when the headphones are unplugged. This may be useful e.g. as a quick and easy means of sounding an alarm in an emergency.

Additionally, to the SMS commands, G Data offers a Web interface from which users can control their devices remotely. To get access to the *Action Center* the user has to register a new account first. Authentication with an existing Internet Security account is not possible.

Anti-Phishing

Internet Security offers real-time web protection against phishing threats for mobile browsers. To use secure browsing, the user has to enable the feature in the settings. When trying to open a phishing site, the browser displays a warning page.

Permissions

The application provides a permission management tool where either apps by permission, or vice versa, can be listed. It is also possible to remove those apps and add them to app protection.

App protection

This feature password-protects selected applications and restricts access to authorized users only. Before app protection is ready to use, it has to be enabled in the settings, and a password needs to be chosen. To protect applications, the user has to hit the *Add* button and select the desired apps from a list.

Parental Control

Internet Security contains a comprehensive parental control feature which allows to define phone usage restrictions regarding time, a set of appropriate applications, web browsing restrictions and pre-set system settings.

Panic Buttons

A panic button can be added as a widget to the home screen. In the process of setting up the button the user can decide which actions it may cause. Available possibilities are an emergency call to a contact from your phone, sending your current location via Email and SMS and sending an Email or SMS with predefined content.

Call Filter

This feature is supposed to block incoming or outgoing calls and texts (the latter not available on Android 4.4 or higher) in a user-defined time period. It is possible to combine contacts into groups and apply filters on them. The application offers an option to block anonymous numbers, but we were not able to make this work in our test scenario.

Hide Contacts

If you don't want others to see some of your phone contacts for whatever reason, you can add them to a feature called "hide contacts" and they will disappear from your contact list. All further communication should only be seen in the Internet Security application. This feature did not work for the contact-related messages in our testing environment, however.

Conclusion

G Data Internet Security is a comprehensive mobile security application that offers lots of functionality to premium subscribers. Most functions, especially its core features, worked as expected and are well implemented. Some minor components are rather inconvenient to use.

Anti-Theft Details		
Commands Web		
Trigger signal tone	✓	Tone not really alarming.
Mute device	✓	
Delete personal data	—	Full factory reset. SD card data can be restored.
Lock screen	✓	Locks the phone.
Set lock screen password	✓	
Locate device	✓	Shown on a Google map.
Commands SMS		
Ring	✓	Ring alarm tone.
Locate	✓	
Locate fine	✓	Provides exact location. Can take longer.
Wipe	—	Full factory reset. SD card data can be restored.
Mute	✓	
Lock	✓	
Set device password	✓	
Remote password reset	✓	Unset Anti-Theft password. Only works if sent from a predefined phone number.

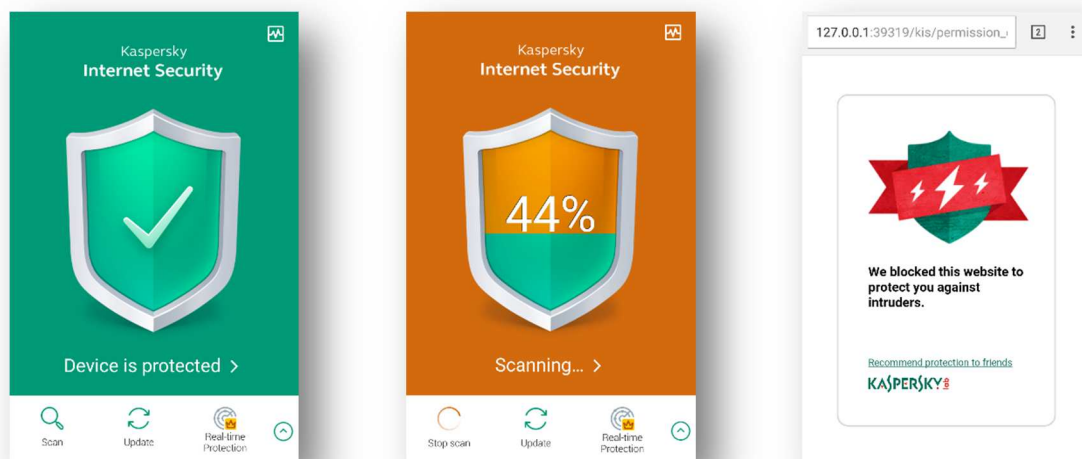


Kaspersky Lab
Antivirus & Security
11.11



Introduction

Kaspersky Internet Security for Android is a mobile anti-virus application that also includes anti-theft features and call/message blocking in the free version. A premium license is available for €10.95 per year and extends the app's functionality with real-time protection, anti-phishing features, and contact hiding.



Usage

After successful installation, the application needs configuration in order to function correctly. Users have to grant some mandatory permissions along with the selection of a country, accepting the license agreement and running an initial scan. Afterwards the application is ready to use.

Antivirus

Kaspersky offers 3 different scan modes including quick scan (installed applications only), full scan (entire device) and scanning a specific directory. Scans can be run manually or prescheduled in a customizable interval. Kaspersky also offers a feature called Real-time Protection, which automatically scans files the user interacts with, and is available in two modes. Recommended Mode checks installed apps only and monitors the download folder. Extended Mode monitors all the user's file activity. Users can decide whether they want

every type of file scanned, or only android apps and archives.

By default, the application tries to disinfect threats detected in any kind of scan. If neutralization fails, the infected files are silently moved to quarantine by default. The quarantine list and the setting the default action for disinfection failure are quite difficult to find. Available actions include moving files to quarantine, deleting or skipping them, or prompting the user to make a decision. The default action for extended Real-time Protection can be set independently. Users can also decide if they want to be protected against potentially unwanted applications (PUAs) and if all files or only archives and applications should be scanned.

Anti-Theft

Anti-Theft configuration requires some device permissions, setting a secret numeric code, and

device admin rights. Through this feature, Kaspersky offers remote control of the device. The feature involves remote device control, a SIM guard, uninstall protection and a web interface. Remote control from other devices is only possible if the counterpart has the application installed. SIM cards could be exchanged at will without the device being locked. Uninstall protection works well, users can who want to remove the application have to do this from the app settings and enter the user's secret code first. Configuration of Anti-Theft settings can be rather annoying since users are always redirected to the start page of the application when pressing the back button. Kaspersky Lab informed us, that the point has been fixed since version 11.12.4.1472 of the product.

Anti-Phishing

The application includes a real-time anti-phishing feature called Web Protection. It protects the user against phishing threats and other malicious content. Users have to enable Web Protection in the application settings before they can surf the web safely. Kaspersky also offers Anti-Phishing protection for text messages, which scans incoming messages for dangerous links.

Privacy Protection

Using Kaspersky Internet Security for Android, it is possible to hide sensitive contact data and conversation history. If users add contacts to a feature called Privacy Protection it is possible to hide data associated with those contacts using a toggle. Contacts can also be hidden using a text-message command or the web interface.

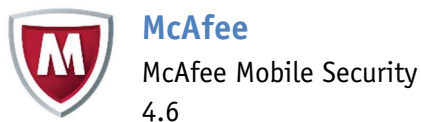
Call & Text filter

Kaspersky's Call Block restricts communication using black- and whitelisting. Users can add numbers to these lists manually or from the call/message log. The filter rules available are rather limited. Users can either block all contacts from the blacklist, allow only numbers from the whitelist or block all unknown numbers. Call & Text Filter also offers the option to block non-numeric numbers.

Conclusion

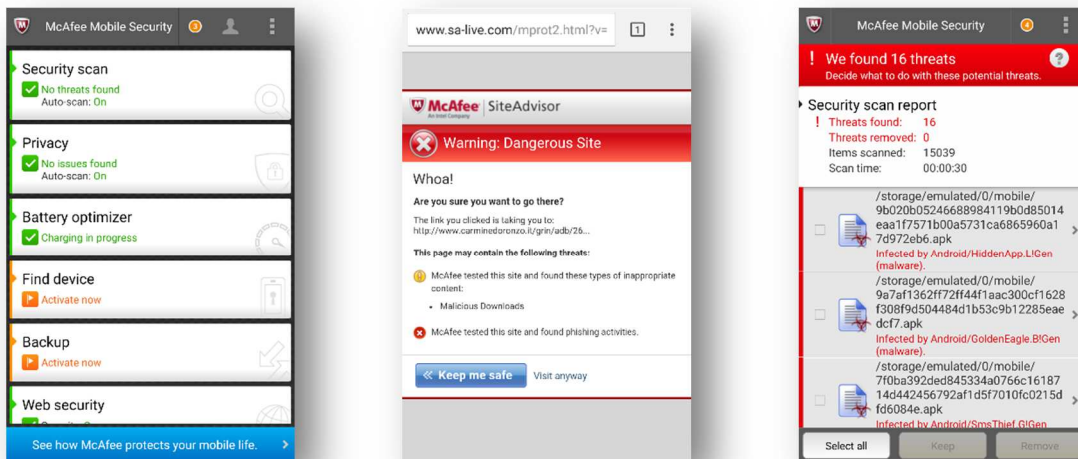
Kaspersky Internet Security for Android is an easy-to-use mobile security app for users who want to install a single application and have done with it. The user interface is simply structured but some specific settings are somewhat hidden.

Anti-Theft Details		
Commands Web		
Lock & Locate	✓	Displayed on <i>Google Maps</i> Map
Mugshot	✓	Takes several pictures
Alarm	✓	
Wipe All Data	—	Factory resets the phone; SD card is not wiped
Wipe Personal Data	✓	As mentioned in the overall report, newer Android versions prevent some data, such as the Google account, from being deleted by any third-party app.
Hide data	✓	Hides contacts listed as sensitive in the privacy protection feature
Text-message commands		
Alarm	✓	
Locate	✓	
Data Wipe	—	As Wipe All Data
Full reset	✓	As Wipe Personal Data
Hide	✓	Hides contact. Reception of command has to be enabled in privacy protection settings.
Additional Features		
SIM Watch	✓	If the SIM card gets replaced, the owner will be informed by a text message to a predefined number. Additionally, the phone can be locked.
Uninstall Protection	✓	



Introduction

McAfee offers a security product which in addition to malware protection and theft-protection also includes backups, a privacy advisor as well as a battery optimizer. The app comes in a free and a premium version, whereby the premium version is ad-free and provides 2GB of cloud space to backup photos and videos and gives access to the McAfee's premium phone support service.



Usage

After the installation the app has to be authorized to access the list of installed apps, and the EULA and Privacy Notice have to be accepted. After that an initial configuration is run by McAfee, and the user is asked to turn on the security features by activating the McAfee's accessibility service.

Security scan

In the security scan window, users are able to start a scan with the pre-defined settings, or update the virus definitions. In the settings there is a way to modify the auto-scan settings, which include toggling real-time scanning, setting a scheduled scan and toggling automatic updates. Additionally, in the scan options the user can decide what should be scanned. This includes apps, potentially unwanted software (PUA), text messages and files. It is also possible to toggle notifications about malicious apps and files.

Under an additional section called Web Security are the phishing and malware protection for the browser. This component also checks for risky Wi-Fi connections.

Find Device

When launching this component for the first time, an initial setup has to be run in order to connect to the web interface. Therefore, a McAfee account has to be created and the necessary permissions have to be granted. Anti-Theft commands can be sent via text messages and a neat web interface. The web interface is basically divided into two parts, which is a bit confusing. There is the modern "Find Device" too, which one is directed to when logging in, and the legacy "My Device". The anti-theft commands can be sent from both, but only the latter provides access to backup data. The old site is not so easy to find, especially as one does not even expect it to be there.

Privacy

The Privacy component is responsible for multiple features. It includes a simple app check (which shows access to private data for certain apps), a call blocker, an app locker, and profiles (which can be used to restrict the apps usable by specific users).

Battery Optimizer

This component is responsible for the speedup tools in the app. One can find an “Extend Battery” function (which turns off some power-intensive setting like Bluetooth), a memory cleaner which kills running tasks, as well as a storage cleaner which can clean the storage from unwanted data like cache files. A data monitor can also be found in this component.

Backup

The Backup component can save private data (text messages, call logs, and contacts) to the cloud and also makes it possible to restore this data. In the pro version the backup of media files is also possible. It is possible to activate automatic backups or to be notified when there is a new contact to be backed up.

Conclusion

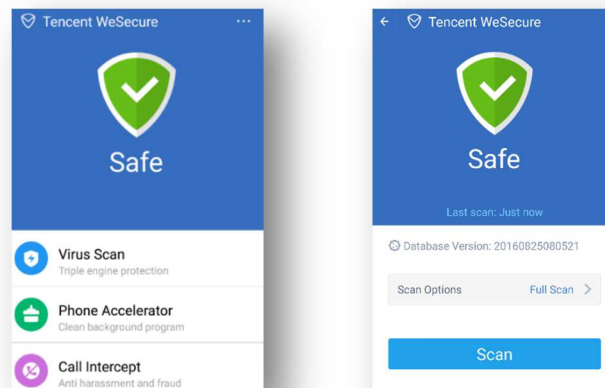
McAfee provides a great security product with good malware detection and a comprehensive anti-theft component. The anti-theft component can be operated via text messages or a good, neat web interface. As already mentioned, this web interface is split up in two parts which makes it a little bit confusing.

Anti-Theft Details		
Commands Web		
Alarm	✓	Plays the device's ringtone
Lock	✓	
Locate	✓	
Capture Cam	—	Tries to take a snapshot of a thief. An alarm is played and a popup message is shown to ensure that the thief is looking at the phone. If the SIM card has been removed from the phone, Capture-Cam fails even if there is Internet access via Wi-Fi.
I lost my device	✓	Triggers lock, locate and capture-cam; if the phone is set to a <i>lost</i> state, the additional actions track, backup, wipe and reset can be used
Track		Tracks the phone for one hour continuously
Backup		Backs up contacts, text messages, call logs and media files
Wipe	✓	Deletes personal data
Reset	✓	Triggers a factory reset of the phone
Commands SMS		
Alarm	✓	Triggers a fairly realistic screaming alarm tone on the phone.
Locate	✓	Sends a link with a map showing the location
Lock	✓	
Reset	✓	
Wipe	✓	
Capture-cam	—	Triggers the capture-cam via a text message.
Additional Features		
SIM Change protection	✓	Locks the device if the SIM card is changed, additionally the user is notified via email
Uninstall protection	✓	Locks the device if device administrator rights are removed from the app
Capture-cam	—	Capture cam takes automatic screenshots when the wrong login credentials are provided for the Android or McAfee lock screen.



Introduction

Tencent WeSecure is an application that primarily focuses on malware protection but also provides several tools that could prove useful when maintaining a mobile device. These tools include Data Backup, Phone Accelerator, and Call Filters. The app is completely ad-free and free of charge.



Usage

On the first start-up of the app, the Terms of Service and Privacy need to be accepted. After that no additional configuration is required and the home screen is shown. The home screen shows the status of the anti-virus component in the form of icon and text. All of the tools provided are listed beneath it.

Antivirus

It is only possible to scan the installed apps on the internal and external storage, or to scan all files on the external drive. The information shown on the screen during a scan is kept neat and simple. The status is shown in the form of icon and text, as on the Home Screen. When malicious files are found, it is possible to remove all of them at once. There is no means of manually updating the signatures, but automatic updates are performed by default.

Phone Accelerator

This tool accelerates the phone's performance simply by allowing the user to close all apps running in the background. However, the feature is poorly implemented. It simply opens

all the Android Internal App Information Pages for the running apps. From these, the programs need to be closed one by one. The component also features sub items for whitelisting and showing running apps.

Call Intercept

This component enables automatic blocking of fraudulent calls and harassment calls, using rules applicable to Chinese telephone numbers. It is not customizable.

Data Backup

The Data Backup component is not included in the main app and needs to be downloaded separately from the app store. It allows the user to back up contacts, messages and call logs.

Conclusion

Tencent WeSecure represents a basic, lightweight anti-virus application, with a data backup feature also included. Tencent users can rely on Android's built-in anti-theft features.



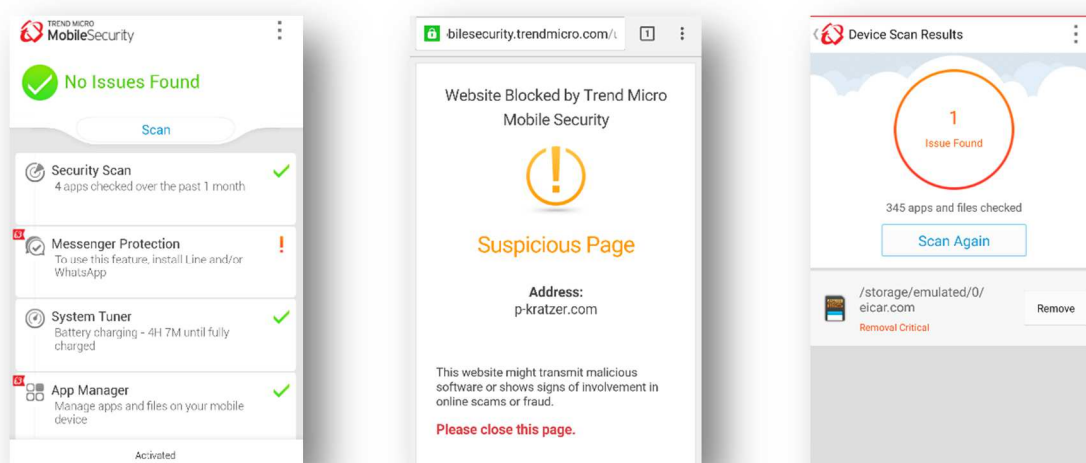
Trend Micro

Mobile Security & Antivirus
8.0



Introduction

Trend Micro Total Security is a comprehensive security app which provides malware detection and several privacy and maintenance tools. The premium version includes a well-designed security concept with advanced features such as pre-installation detection via VPN, and messenger protection for Line and WhatsApp.



Usage

After installation, terms of use need to be accepted, and the user has to decide whether to send anonymous usage reports. The home screen provides the overall security status, as well as the status of every component next to its name. After installation, for example, any missing permissions are displayed there. By tapping the *Scan Device* button on the home screen, the user can run a check for malware and privacy risks. The app features scanning for malware, privacy issues such as Facebook settings, and app-management and system-tuning tools. Anti-theft, call-blocking and safe-surfing tools are also implemented. These components are, in contrast to other functions, all integrated by default.

Security Scan

A scan can be started either directly from the home screen of the app, or from the security scan menu. The app provides a number of scan options for malware e.g. Real-Time Scan, Pre-Installation Scan and a full scan including the SD card. The user can scan just apps or all files. There are various settings for updates as well, such as manual updating, and scheduling a scan after every update.

When malware is found during a scan, the app reports it on multiple ways, such as pop-up notifications and the indicator on the home screen. To use Pre-Installation Scan, a VPN connection has to be set up, which will scan the network traffic and warn for malicious apps downloaded from the Google Play store. To do this, the Trend Micro Security Certificate has to be installed on the phone.

Lost Device Protection

Lost Device Protection provides the anti-theft component of the app, which is controlled via a web interface. The message which is shown when the device is locked, as well as for wipe mode (factory reset or only personal data), has to be set in the app. These decisions cannot be made from within the web interface. Besides the obligatory functions such as alarm, find, wipe and lock, the position of the device can be shared via Facebook.

Network Protection

The network protection component provides a safe surfing component which will warn of malicious sites while surfing the web, as well as a Wi-Fi checker which warns of unsecure Wi-Fi connections. The protection level for safe surfing can be set to low, which will only block reported fraudulent sites, high, which will block all sites with any fraudulent or malicious signs, or normal, which provides a balanced level of protection that does not block minor risks. Additionally, to the automatic protection, sites can be whitelisted/blacklisted, and Wi-Fi Hotspots can be added to a trusted Wi-Fi list.

Messenger Protection

Messenger Protection can scan messages in Line and WhatsApp, and warns for malicious links. The protection level for safe-surfing is automatically applied to Messenger Protection, which is very convenient.

Parental Controls

Parental Controls provides an app lock and a website filter to protect children from inappropriate content. The website filter can be set to three different profiles (Child, Pre-Teen and Teen) which will filter content appropriately for the age group. Blocked sites can be seen in a log, and it is also possible to whitelist/blacklist individual sites manually.

Call Blocking

The call blocking feature supports blacklisting or whitelisting and can optionally reject the call, silence the phone or reject the call and answer with a customizable text message.

Additional Features

In addition to the standard components of a security app, Trend Micro provides a System Tuner which provides battery and memory optimisations, an app manager that lists installed applications, and a Facebook scan which scans one's privacy settings for Facebook.

Conclusion

Trend Micro's Mobile Security for Android is a comprehensive app that provides an advanced security concept. In our test, all the features worked conveniently and provided a great user experience. Even though the lost-device protection was easy to use, text-message commands would be nice to have.

Anti-Theft Details		
Commands Web		
Locate / Track	✓	Displayed on a <i>Bing Maps</i> map
Lock	✓	
Wipe (factory reset)	—	The external SD card was not wiped.
Wipe (personal data)	✗	The external SD card was not wiped. Browser history and Google account were not removed. The Trend Micro account was removed, which makes future commands impossible.
Alarm	✓	
Share Location on Facebook	✓	Creates a post with a link
Additional Features		
SIM Change Protection	✓	Locks the device if the SIM-card is changed or removed; device is unlocked automatically if the original SIM is inserted again
Uninstall Protection	✓	Part of the Parental Controls component

Feature List Android Mobile Security	FREE	FREE	FREE	COMMERCIAL	FREE	COMMERCIAL	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	FREE	COMMERCIAL
Product Name	Android OS	Alibaba Ali Money Shield	Antiy AVL for Android	Avast Mobile Security & Antivirus	Avira Antivirus Security	AVG AntiVirus PRO	Baidu Mobile Guard	Bitdefender Mobile Security & Antivirus	ESET Mobile Security & Antivirus	G Data Internet Security	Kaspersky Internet Security	McAfee Mobile Security	Tencent WeSecure	Trend Micro Mobile Security & Antivirus
Version Number	6.0.1	5.0.1	4.6	5.2.0	4.5	5.4.1	8.3.0	3.0	3.3	25.10	11.11	4.6	3.4	8.0
Supported Android versions	built-in	2.2 and higher	2.1 and higher	2.2 and higher	2.2 and higher	2.2 and higher	2.2 and higher	2.3.3 and higher	2.3 and higher	2.1 and higher	2.3 and higher	2.3 and higher	2.1 and higher	2.3 and higher
Supported Program languages	All	Chinese	English	English, Czech, French, Italian, Spanish, German, Russian, Portuguese, Catalan, Hungarian, Dutch, Polish, Turkish, Vietnamese, Chinese, Japanese, Bulgarian	English, German, French, Italian, Spanish, Korean, Japanese, Portuguese	English	Chinese	English, Portuguese, French, German, Italian, Polish, Romanian, Spanish, Turkish, Vietnamese	English, Polish, Danish, Finnish, Norwegian, Japanese, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Swedish, Chinese, Italian, French, Korean, Czech, Hebrew, Slovak, Vietnamese, Arabic, Bulgarian, Thai	German, English, French, Spanish, Portuguese, Italian, Dutch, Polish, Russian, Turkish, Japanese, Chinese	English, Russian, German, French, Spanish, Italian, Portuguese	English, Danish, German, Greek, Spanish, Finnish, French, Indonesian, Italian, Japanese, Korean, Norwegian, Dutch, Portuguese, Russian, Swedish, Turkish, Chinese	Chinese	English, German, Spanish, French, Italian, Korean, Dutch, Portuguese, Chinese, Turkish, Vietnamese
Anti-Malware														
On-Install scan of Installed apps	•	•	•	•	•	•	•	•	•	•	•	•	•	•
On-Demand scan		•	•	•	•	•	•	•	•	•	•	•	•	•
On-Access scan for files		•	•	•	•	•	•	•	•	•	•	•	•	•
Scan works offline		•	•	•	•	•	•	•	•	•	•	•	•	•
Scan is assisted by cloud	•			•	•	•	•	•	•	•	•	•	•	•
Automatic (scheduled) Scan			•	•	•	•	•	•	•	•	•	•	•	•
Scan installed apps for (possible) privacy violations	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Safe Browsing (Anti-Phishing & Anti-Malware)	•		•	•	•	•	•	•	•	•	•	•	•	•
Recommendations for android settings	•	•		•			•	•	•	•	•	•	•	•
Quarantine									•					
USSD Blocking	•	•		•	•				•		•	•		
Anti-Theft														
Remote Locate, Alarm, Lock & Wipe	•	•		•	•	•	•	•	•	•	•	•	•	•
Webinterface for controlling Anti-Theft features	•	•		•	•				•		•	•	•	•
SMS commands for controlling Anti-Theft features				•	•				•		•	•	•	•
Notify on SIM Change (Email / SMS)				•	•			•	•		•	•	•	•
Lock on SIM Change			•	•	•			•	•		•	•	•	•
Remote Unlock				•	•		•		•		•	•	•	•
Anti-Spam														
Whitelist / Blacklist Phonecalls		•		•	•		•		•		•	•	•	•
Whitelist / Blacklist SMS		•		•	•		•		•		•	•	•	•
Whitelist / Blacklist with wildcards				•	•				•		•	•	•	•
Blocking of SMS containing keywords		•					•				•	•	•	•
Parental Control														
Safe Webrowsing				•				•		•		•		•
Lock Apps			•	•		•		•		•		•	•	•
App launcher especially for kids (Parents can choose apps)										•		•		
Authentication														
Uninstallation protection (password required for uninstallation)				•		•		•	•	•	•	•	•	•
Settings protected with password				•		•		•	•	•	•	•	•	•
User Account needed to use product	•				•			•	•	•	•	•	•	•
Additional features														
Backup	•			•		•		•		•		•	•	•
Local Wipe	•			•		•		•			•	•	•	•
Network monitor				•		•		•	•		•	•	•	•
Task Killer	•			•		•		•			•	•	•	•
Battery Monitor	•					•			•			•		
Support														
Online Help & FAQ	•			•	•	•	•	•	•	•	•	•	•	•
Email support		•	•	•	•	•	•	•	•	•	•	•	•	•
User Forum	•			•	•	•	•	•	•	•	•	•	•	•
User Manual	•			•	•	•	•	•	•	•	•	•	•	•
Phone Support				•	•	•	•	•	•	•	•	•	•	•
Online Chat								•	•		•	•	•	•
Supported languages of support	All	Chinese	English, Chinese	English, Czech, French, Spanish, Portuguese, Turkish, Polish, Russian, German, Chinese, Italian	German, English, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malaysian, Korean	English, German, Czech, French, Italian, Dutch, Polish, Spanish, Portuguese	Chinese	English, French, Italian, Spanish, Portuguese, Romanian, German, Turkish	All	German, English, Spanish, Italian, French, Portuguese, Chinese, Japanese	English, Russian, German, French, Spanish, Italian, Portuguese	Spanish, English, Portuguese, Czech, Danish, German, French, Chinese, Italian, Japanese, Dutch, Norwegian, Polish, Russian, Suomi, Swedish, Turkish, Korean	Chinese	English

Copyright and Disclaimer

This publication is Copyright © 2016 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives (September 2016)