

# AV-Comparatives



## Mobile Security Review

Language: English

September 2014

Last revision: 29<sup>th</sup> September 2014

[www.av-comparatives.org](http://www.av-comparatives.org)

# Contents

Introduction .....	3
Overview .....	5
Products tested .....	7
Battery usage.....	8
Malware protection results .....	10
AVC UnDroid Analyser.....	10
Android Device Manager .....	12
AhnLab V3 Mobile .....	13
avast! Mobile Security .....	17
Avira Antivirus Security .....	22
Baidu Mobile Security.....	26
Bitdefender Mobile Security.....	29
CheetahMobile Clean Master .....	33
CheetahMobile CM Security.....	36
ESET Mobile Security .....	39
F-Secure Mobile Security .....	43
G Data Internet Security .....	46
Ikarus mobile.security .....	50
Kaspersky Internet Security.....	53
Kingsoft Mobile Security .....	57
McAfee Mobile Security.....	60
Qihoo 360 AntiVirus .....	64
Quick Heal Total Security .....	67
Sophos Security and Antivirus.....	72
Tencent Mobile Manager .....	76
Trend Micro Mobile Security.....	80
Webroot SecurityAnywhere Mobile Complete	84
Summary .....	87
Appendix - Permissions.....	88
Appendix – Feature list.....	89
Copyright and Disclaimer .....	90

## Introduction

Smartphones represent the future of modern communications. In 2013, more than 1 billion smartphones were sold, a further milestone in the advance of these devices<sup>1</sup>. A study published by Facebook emphasises the importance of smartphones in our lives; about 80% of users make use of their smartphone within 15 minutes of waking up each day<sup>2</sup>.

At the same time, the traditional function of a telephone is becoming less and less important. The high quality of integrated cameras means that the smartphone is increasingly used for photography. As well as with photos, users trust their devices with their most personal communications, such as Facebook, WhatsApp and email. This brings some risks with it, as such usage makes the smartphone interesting for criminals, who attempt to infect the device with malware or steal personal data. There is also the danger brought by phishing attacks.

These days, the use of security software on a PC or laptop is seen as essential. However, many smartphone users do not yet have the same sense of responsibility, even though their devices store personal data, private photos, Internet banking information or even company data.

As modern smartphones are often expensive to buy, they are also an attractive target for thieves. Top-quality smartphones cost several hundred Euros. As it is not possible to physically prevent them from being stolen, they must be made less attractive to thieves. Consequently, many of today's security products contain not only malware protection, but also highly developed theft-protection functions, which make the device less attractive to thieves (e.g. by locking the device), and help the owner to find it again.

This year, we have once again tested security products for smartphones running Google's Android operating system. Our report covers details of the products made by leading manufacturers who have agreed to participate in our review. The test was conducted in July and August 2014 on an LG Nexus 5 smartphone running Android 4.4.2. In the event that a function did not work properly, we then installed the product on a Samsung Galaxy S3 Mini with Android 4.1.2 and repeated the test. This verifies whether the malfunction is a general one, or is limited to the newer Android version. We also tested the "wipe" function (deletion of personal data) of each applicable product on the alternative device, with particular regard to the deletion of data on the external SD card. This was necessary, as the Nexus 5 does not allow an external SD card to be used.

In general, we found that the current Android version, 4.4, clearly has problems with text-message blocking features in security products. None of the products we tested was able to make this work. Many manufacturers warn the user of this. Text messages cannot be blocked or hidden under Android 4.4. This is particularly problematic for products that use text-message commands to control their features. Thieves are able to see text messages in plain text, meaning that they can see the password. We thus recommend sending a "lock" command first, before using other features such as locating or wiping the device. This is the only way the user can ensure that a thief does not have access to his or her texts.

Security software for Android usually requires a wide range of operating-system permissions, which we granted, to ensure that the program would work properly. We noticed a high degree of variation between products, however. We decided to publish a table in this year's report that displays all the permissions required by each product. This can be seen in the appendix on page 87.

---

<sup>1</sup> <http://www.dw.de/2013-%C3%BCber-eine-milliarde-smartphones-verkauft/a-17391228> (German)

<sup>2</sup> <https://fb-public.app.box.com/s/3iq5x6uwnqtq7ki4q8wk>

## Theft Protection

Almost all the products in the test provide a theft-protection feature. The lock function is surely the most important. This protects the phone from unauthorised use by password protecting it. Remote deletion of personal data on the smartphone is also a standard feature of the tested programs. The position of the phone can be determined by a location function. This can be helpful in locating a lost phone, although some manufacturers explicitly warn against confronting a thief.

Manufacturers have two possible means of controlling their theft-protection software. One is text-message commands, which are sent to the lost or stolen phone and set off the relevant functions. The other is a web interface. Each has its own advantages and disadvantages. The advantage of text-message commands is that they almost always work, even if the device is in another country. The user needs to have the commands to hand, however, and also requires access to another mobile phone in order to send them. By contrast, web interfaces are generally intuitive in use, and provide an easy means of controlling the device. The disadvantage is that the lost or stolen device requires an active Internet connection in order to work; this may well be deactivated if the phone is taken to another country. The location function could also be to locate the *person* carrying the phone, which in some cases could constitute misuse. It is possible to install a security product on someone else's phone, or give someone else a phone with the software already installed, in order to track that person's movements. This may be deemed legitimate in the case of parents keeping an eye on their children, but not necessarily in other cases.

The Android operating system has a basic but reliable theft-protection feature, called Device Manager, built in to it. We have also tried out the available functions of Android Device Manager, to provide readers with the most complete view of available software. The review of the available functions can be found on page 122. A general problem regarding theft-protection, which affects many products, is airplane mode. This can be activated even when the smartphone is locked. If this mode is activated, all contact with the outside world is lost, thus rendering theft-protection mode completely ineffective. Not all the functions, such as locking, wiping and locating, will work. This applies equally to text-message controls and the web interface.

## Malware protection

This component scans the mobile phone for malicious software, which it deletes or quarantines. For this function to work effectively, it has to be kept up-to-date. When travelling abroad, users need to be careful that automatic updates and cloud scans do not incur high roaming costs from the mobile service provider. The results of our Android malware protection test can be seen on page 11.

## Battery usage

Many smartphone users will have found themselves in a position, usually towards the end of the day, in which they wished they had a portable power station with them. The multiple functions of smartphones mean that even energy-efficient smartphones cannot prevent substantial battery-usage. GPS location services, email, Internet, and the larger displays in modern smartphones result in the device eating up the power. If the smartphone is used intensively, the battery can be run down by the afternoon. To prevent this, there are three possibilities: strictly controlled use of the phone, carrying a portable charging device, or configuring the device to use as little power as possible. Many users still believe that security software makes high demands on the battery of an Android smartphone. Our battery-usage test found that in everyday use of the phone, the influence of security products on battery life is negligible. Running backups, updates and malware scans does lead to significantly higher battery usage, however. Some products get around this by allowing the user to configure the software so that these functions are only carried out when the smartphone is being charged.



## 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 many of the tested products. The manufacturers of the affected products have taken these problems very seriously and are already working on solutions. Overall, we have noticed a marked improvement in the quality of the products relative to last year. We are therefore pleased to give almost all the participating products our “Approved Award”. Unfortunately, it was not possible to give this award to Tencent’s security app, due to its score in the malware protection test. Qihoo has also not been awarded, as their tested product version is currently no longer available and not the same as in the Google playstore.



**AhnLab V3 Mobile** provides the most important security functions for Android. Additional features include file encryption and a network monitor.

This year’s version of **avast! Mobile Security** has been extended to include Applocker and Privacy Scan features. It is a very comprehensive security product with a wide range of configuration options.

**Avira Antivirus Security** is an attractively designed security app for Android, and provides all the important functions. The theft-protection feature is controlled by a web interface. Innovative components such as Identity Safeguard complete the product.

**Baidu Mobile Security** is an extremely easy-to-use security product for Android smartphones. It provides many features, such as optimisation functions, an app manager and anti-spam.

**Bitdefender Mobile Security** has been optically redesigned since last year, and now includes an app blocker. The features are well thought-out, and generally worked very well.

**CheetahMobile** aims to digitally clean the mobile phone with **Clean Master**. As well as a virus scanner, there are other functions such as RAM/storage cleaning.

**CheetahMobile CM Security** is a solidly implemented security product for Android smartphones, which provides important functions such as antivirus and theft protection.

**ESET Mobile Security** is a well thought-out and attractively designed product for Android smartphones. The functions are solidly implemented and performed well. This year’s version has been extended to include a web interface for the theft protection.

**F-Secure Mobile Security** is a security package that includes important features such as theft protection and malware scanner. Parental controls and safe surfing are also provided.

**G Data Internet Security** provides sophisticated protection for children in addition to the standard security features. This includes Children's Corner and a special browser for children.

**IKARUS mobile.security** includes all the important security features. The user interface is very clearly laid out, and should be simple to use for everyone. The components included generally worked well.

**Kaspersky Internet Security** has been optically reworked since last year. It has a comprehensive range of features, including virus scanner, text-message and call filter, browser protection, theft-protection and more.

**Kingsoft Mobile Security** for Android available free of charge, and optically very simple. As well as traditional malware protection, there are additional features such as a spam filter for text messages, and battery-life protection.

**McAfee Mobile Security** is a well thought-out suite, which as well as the usual functions also includes features such as CaptureCam and Kids' Corner.

Last year's version of **Quick Heal Total Security** was already rich in functionality, and this year is again one of the most comprehensive products. The current version has also been given an optical makeover.

**Qihoo 360 AntiVirus**, which was only available in Chinese last year, participates in this year's test with the new English version. Important functions are included, along with innovative features such as Anti-Adware. The result reached in this test by Qihoo is not applicable to the English product version available in the Google playstore. Due to the misuse of the award by Qihoo in their related marketing, the award has been withdrawn.

**Sophos Security and Antivirus** provides useful features that actively promote the user's security. The Security Advisor, which checks critical settings, is of particular note, as is the well-designed Spam Protection component.

**Mobile Security** by **Trend Micro** provides sensible extensions such as safe surfing and well-implemented parental controls, in addition to the usual functions of theft protection and malware scanner.

**Tencent Mobile Manager** is a security product for Android with extensive functionality. There is a wide range of optional add-ons available, which can extend the product even further. Due to the score in the malware-protection test, which according to Tencent was due to a bug in the product at the time of testing, we are unfortunately not able to approve the product.

**Webroot SecureAnywhere Mobile Complete** scores highly with its reliable theft protection and text/call filter. The premium version additionally includes SIM lock, app inspectors and other functions.

## Products tested

The products that participated in this year's test are listed below. The manufacturers either provided us with the latest version of their product, or confirmed that it was available from the Google Play Store at the time of the test (July 2014). After the test, manufacturers had the opportunity to fix any flaws we found. Any problems that have already been solved are noted in the report.

- AhnLab V3 Mobile 2.1.2.13
- avast! Mobile Security 3.0.7650
- Avira Antivirus Security 3.5.2983
- Baidu Mobile Manager 5.2.0
- Bitdefender Mobile Security 2.19.344
- CheetahMobile Clean Master 5.6.0
- CheetahMobile CM Security 1.6.1
- ESET Mobile Security 3.0.937.0-15
- F-Secure Mobile Security 9.2.15183
- G Data Internet Security 25.3.0
- IKARUS mobile.security 1.7.20
- Kaspersky Internet Security 11.4.4.232
- Kingsoft Mobile Security 3.3.1
- McAfee Mobile Security 4.1.0.543
- Quick Heal Total Security 2.00.021
- Qihoo 360 AntiVirus 1.0.0
- Sophos Security and Antivirus 3.5.1324
- Tencent Mobile Manager 4.8.2
- Trend Micro Mobile Security 5.0
- Webroot SecureAnywhere Mobile Complete 3.6.0.6610



The mobile products of **Baidu**, **Kingsoft** and **Tencent** are currently only available as Chinese-language versions. The result reached in this test by **Qihoo** is not applicable to the English product version available in the Google playstore, which is different to the version that Qihoo provides in Chinese and English on their website.

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/>

## Battery usage

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 many 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.

In April 2012, AV-Comparatives conducted a survey of smartphone use, in order to optimise the testing procedure. Over a thousand smartphone users from around the world were asked to anonymously answer questions about their smartphone use. It was apparent that the respondents made good use of their smartphones' features. 95% of users surveyed said that they use their phones to surf the Internet and communicate by email, whilst over two thirds listen to music or watch videos on their mobiles. It was notable that 70% of the users never switch their phones off.

Smartphones are becoming more and more important to their users, who scarcely leave any functions of their devices unused. The mobile phone is a ubiquitous means of communication that is supplementing or even replacing the personal computer.

Telephony is becoming a less important use of the smartphone, with 41% of survey respondents saying they only used the device for 1-10 minutes each day. Most users spend longer than this on the Internet; over 29% for over an hour a day.

We used the 2012 survey as the basis for our usage statistics in the battery drain test. The data was used to define average daily use of a smartphone. The test then determined the effect of the security software on battery use for the average user.

## Environmental conditions

To measure the battery drain as accurately as possible, we used an ISO-calibrated measuring device, in co-operation with Agilent and x-test. The highly accurate battery-drain meter allows very precise measurements to be taken. An automated process, emulating the typical usage as established in the survey, is run multiple times.

## Outside influences

In order to exclude any influence from environmental conditions or technical variations, we took great pains to ensure that the testing conditions for each product were identical, in accordance with ECMA-383<sup>3</sup>.

3G connections and WiFi connections can vary according to e.g. weather conditions. In order to prevent such variations influencing our test, we set up our own WiFi base station and UMTS base station in our testing lab. This ensured that the energy expended in supporting the 3G/WLAN connection was the same for every product.

These values are of course also influenced by the mobile phone used. Multiple factors come into play here. For example, a large screen will require more energy than a small one. The type of screen (e.g. LCD, OLED, AMOLED) is also highly relevant. By using the same individual device for all test candidates, we were able to rule out any such influences.

---

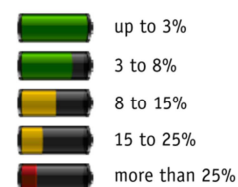
<sup>3</sup><http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-383.pdf>

Based on the survey data, the following daily usage scenario was simulated:

- 30 minutes **telephony**
- 82 minutes **looking at photos**
- 45 minutes **surfing the Internet** with the Android browser (using web pages on a local web server to rule out any influences through connection speed)
- 17 minutes **watching YouTube videos** with the YouTube app
- 13 minutes **watching videos saved on the phone itself**
- 2 minutes **sending and receiving mails** with the Google Mail Client
- 1 minute **opening locally saved documents**



Manufacturer	Battery usage	Manufacturer	Battery usage
AhnLab		Ikarus	
avast!		Kaspersky Lab	
Avira		Kingsoft	
Baidu		McAfee	
Bitdefender		Qihoo	
Cheetah Mobile C.M.		Quick Heal	
Cheetah Mobile CM S.		Sophos	
ESET		Tencent	
F-Secure		Trend Micro	
G Data		Webroot	



Overall, the security suites performed well in this test. However, one of the products did cause higher battery usage, namely **Baidu**. We were not able to find a particular operation for which the product used more energy, but overall its battery usage was higher.

## Malware protection results

Methods of attacking mobile phones are getting more and more sophisticated. Fraudulent applications attempt to steal smartphone 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 Sideloading<sup>4</sup>. 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 great is the risk of infection with an Android smartphone?

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 lower than in many Asian countries, especially China. There are many rooted phones and unofficial app stores, which increase the chance of installing a dangerous app. In many Asian countries the smartphone is used as a replacement for the PC, and is frequently used for online banking. Banking apps are also becoming more popular in Europe and the USA. There is a high risk involved in receiving the mTan code on the same phone that is used to carry out a 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/>

---

<sup>4</sup> <http://en.wikipedia.org/wiki/Sideloading>



## Test Set

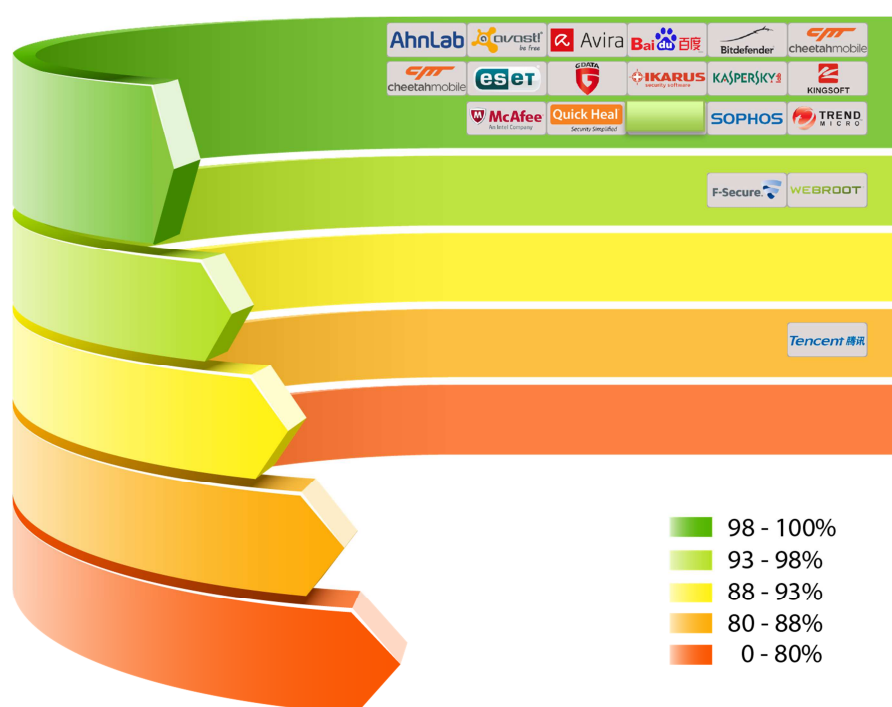
We collected the malware samples used in the test during the period of few months leading up to the test. **3991** malicious applications were used to create a representative test set. So-called "potentially unwanted apps" were not used in the test. The security products<sup>5</sup> were updated and tested on the 11<sup>th</sup> July 2014.

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 manually. We did this to allow the products to detect the malware using real-time protection.

We additionally conducted a false-positive test using the top 100 ad-free programs from the Google Play Store. None of the products tested produced any false positives with these apps.

## Protection rate results

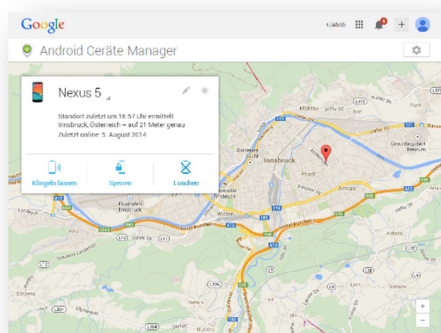
1. AhnLab, G Data	100%
2. Avira, Bitdefender, McAfee, Cheetah Clean Master, Cheetah CM Security, Kingsoft, Trend Micro	99,9%
3. Avast	99,8%
4. ESET, Kaspersky Lab	99,7%
5. Quick Heal	99,5%
6. Ikarus	98,9%
7. Baidu, Sophos	98,8%
8. Webroot	97,4%
9. F-Secure	96,1%
10. Tencent	83,8%



<sup>5</sup> The result reached by Qihoo in this test is not applicable to the English product version available in the Google playstore, which is different to the version that Qihoo provides in Chinese and English on their website. Therefore the results of Qihoo are not shown here.

## Android Device Manager

The Android Device Manager provides the user with solid base functionality with regard to theft protection, and is installed by default in the Android operating system. The component is controlled by a web interface: <https://www.google.com/android/devicemanager>. Text-message commands are not available.



### Installation

No installation is required, as the protection is built into Android. On our test device, the component was already activated. In some cases, it may need to be enabled in the settings.

### Locate

This function locates a lost or stolen phone and shows its position in Google Maps. Only one location is shown at a time; tracking the movement of the phone is not possible.

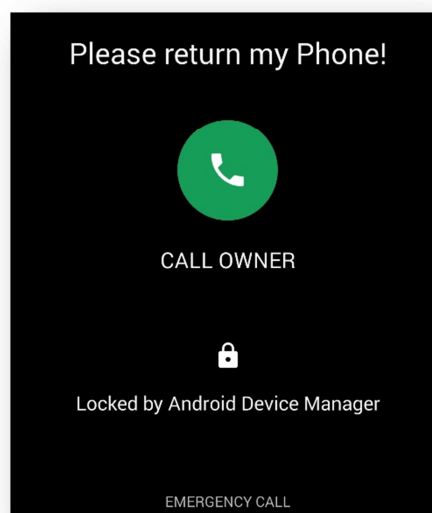
### Ring

The Ring function sounds a melody at full volume for five minutes. This allows the owner to find the phone if it has been mislaid. The command does not lock the phone.

### Lock

The Lock function uses the Android lock screen to lock the device. This makes it inaccessible to unauthorised users. The password for the lock screen can be set in the web interface. We liked the fact that a message is displayed on the lock screen, which can likewise be defined in the web interface. This allows information to be

displayed that would let an honest finder contact the device's owner in order to return it. To this end, a telephone number can be additionally displayed. The lock screen allows this number (and this number only, except emergency calls)



In our test, the lock functioned exactly as it should. We were not able to bypass it, and an emergency call was possible at all times.

### Wipe

This function deletes personal data from the user's smartphone. Once the command has been received, the device is returned to factory settings. Google points out that on some devices, the SD card will not be wiped under some circumstances. We were able to confirm this in our tests. Whilst on our Nexus 5 all data was deleted, including from the SD card, the command did not wipe the SD card on our alternative test device with the older Android version.

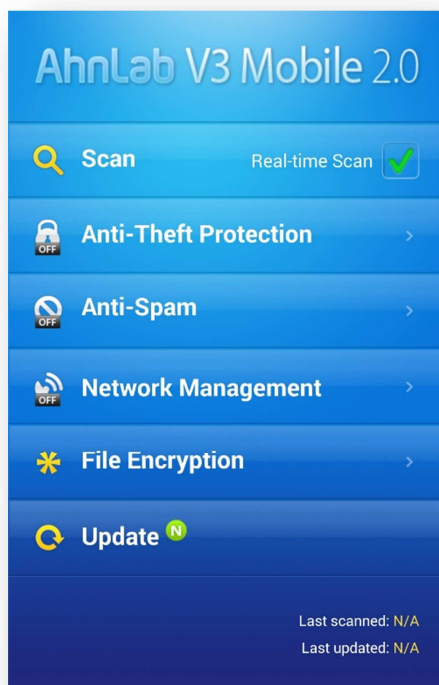
### Summary

Google's Android Device Manager does not offer a great range of functionality, but all the available components are very effective. For users who principally want the theft-protection features of a mobile security product, the Android Device Manager could be a good choice.



## AhnLab V3 Mobile

AhnLab's V3 Mobile is a security product for Android that contains the most important security features, such as a malware scanner, theft protection and anti-spam.



### Installation

AhnLab provided us with an APK file for the test. The installation process is simple. Once the licence agreement has been accepted, the device has to be registered. This is completed in a few seconds, without any additional details needing to be entered. The user is then taken to the product's start screen.

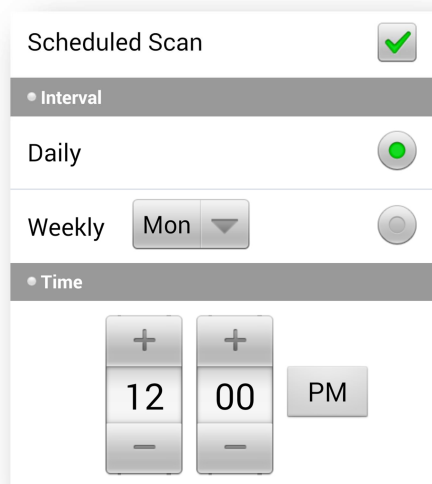
### Starting the program

Once it has been successfully installed, AhnLab V3 Mobile can be started. There is no form of introductory tutorial, so the user must explore the product to find out how it works. An initial update is not carried out. The real-time protection, which is activated by default, can be switched off and on directly from the home screen. All other components can be found in the same place. The details of the last scan and last update are displayed along the bottom edge of the screen. Initially, "N/A" is shown.

### Scan

Two forms of check are offered by the Scan module. There is the "Smart Scan", which checks all installed apps for malicious behaviour, and the "Intense Scan", which additionally scans all files on the device. The details of the last scan carried out, and the next scheduled scan, are displayed. Settings for this are set in the global configuration menu. As well as the interval (daily or weekly), the time of day can be set.

Another option in the settings is whether "Potentially Unwanted Apps", i.e. apps that users possibly do not wish to install on their devices, should be blocked. AhnLab suggests adware, spyware and dialers as examples of such applications.



### Theft protection

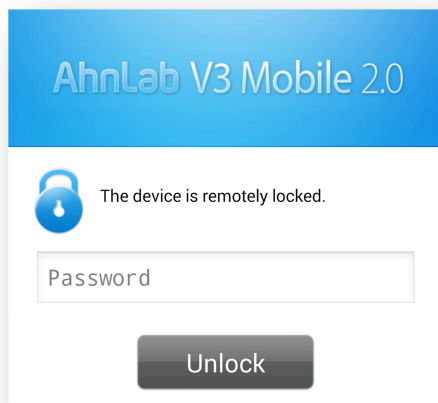
To use this feature, the user has to enter a password with between 4 and 8 characters. Additionally, the product must be made a Device Administrator. Overall, the setup process is very simple. AhnLab uses text-message commands to control the theft-protection component; an overview of these is shown. Using an entry line, the user can check the correctness of text commands and test them straight away. A web interface is not provided.

## Lock

### Text-message command:

**"#lock <password><message>"**

This function locks the smartphone, securing it against unauthorised usage. The password (previously configured) has to be entered to unlock the phone. We liked the fact that a personal message can be displayed on the screen. Another plus point is the fact that after ten failed password entries, a text message with the phone's location is sent to the phone used to initiate the lock command.



However, we also have to note some minus points. When the phone has been locked, it is no longer possible to make emergency calls from it. In addition, the lock screen is not very secure. Simply pressing the Home button displays the Android start screen. This can be used to navigate and show the installed apps. Programs can also be started, although the lock screen is shown again after a few seconds. In our test, we were able to navigate to the text message containing the lock password. The lock component is thus not fit for purpose.

### Remote Data Delete

**SMS command: "#remove <password>"**

This command deletes personal data from the smartphone. The device is not reset to factory defaults, which has the advantage that the anti-theft software is not removed, and so its functions remain active. Although the text messages were not removed, the component largely worked well. All contacts, files,

calendar entries, browser history and bookmarks were deleted.

In a second test, using a different device with Android 4.1.2, the text messages were erased too. However, PDF and ZIP files were not deleted from the external SD card on the 4.1.2 device. Media files such as JPG, MP3, MP4 and AVI were successfully deleted; However, we were able to restore a majority of all deleted files on the external SD card using a freeware tool.

### Remote Wipe Reset

**Text-message command: "#kill <password>"**

This command resets the device to factory defaults. In contrast to the Remote Data Delete function, text messages on the device are deleted too. However, there is the disadvantage that the theft-protection components are also removed.

### Remote Location Tracking

**Text-message command: "#locate <password>"**

When this command has been transmitted, the sender's phone will receive a prompt reply containing a link to the phone's position in Google Maps, along with co-ordinates. Although we understand the term "tracking" to mean continuously locating the device over a longer period of time, the feature actually performed very well.

### SIM card swap

If the SIM card is swapped, a text message with the device's location will be sent to the number specified by the user during setup. The device will also be locked.

In our test, this feature did not work. No text message was sent, and the device was not locked. However, in a second test on a device running Android 4.1.2, the feature worked as expected.

### Anti-Spam

AhnLab's Anti-Spam component allows calls and texts from specific phone numbers to be blocked. A number of ways of adding numbers to the blacklist are provided. Numbers to be

blocked can be added from call and text-message logs, the contact list, or by entering manually. For each individual number, it is possible to block only calls, only texts, or both.

Text messages can also be blocked according to their content. Keywords of between two and ten characters can be defined for this purpose. It is not clear to us why the word length is limited. A sub-menu entry displays all calls and texts that have been blocked previously. We note that the word-blocking is case-sensitive; we do not understand the sense in this.

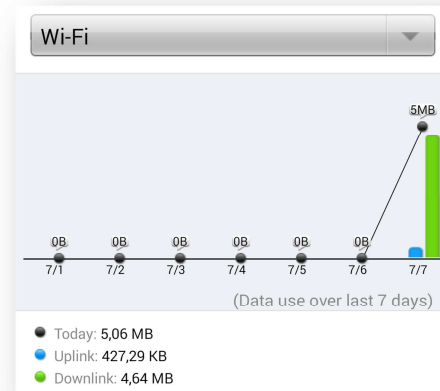
However, we would describe the Anti-Spam component as well-designed and clear overall. Call blocking functioned perfectly, although text-message blocking did not work in this year's test. It would appear that the product has problems with the Android version used in the test (4.4.2); as noted above, the text-blocking function worked as expected with Android 4.1.2.

### Network Management

AhnLab bundles together all network-related functions under Network Management.

When the device is connected to a wireless network (WLAN), a pop-up message box appears that allows the user to deactivate WiFi, remember the current connection, or to block it. Known wireless access points can be managed using a list.

Data usage over mobile networks can be limited. When usage has reached a pre-defined limit, the user is warned. The Network Monitoring page displays data-usage statistics. These can be sorted according to connection type, i.e. mobile or wireless. Data usage can also be displayed according to whether the data was downloaded or uploaded.



### File Encryption

File Encryption allows individual files to be encrypted. A file manager allows multiple files to be selected and encrypted with an alphanumeric key. The result is a file with an AED extension, which cannot be opened unless decrypted; this is also carried out using the AhnLab application. There are no limitations on the type of file that can be encrypted, so pictures, videos, PDF files and so on can all be secured. In our test, the files were correctly encrypted and decrypted, but the application crashed after each procedure.

### Updates

Updates can be installed manually or set to run on a schedule. The user can decide whether to download these exclusively over WiFi, or use the mobile phone network as well.

### Help

AhnLab provides a very well-ordered help function. We particularly liked the step-by-step instructions. We were however irritated by the fact that pressing the Back button returns the user to the start screen or start of the help. There is also no zoom function, which is a shame, as all the text is very small.

### Deinstallation

There is no uninstall wizard provided, but there is a step-by-step guide in the help. To start with, AhnLab V3 Mobile must be removed from the list of Device

Administrators. The Android App Manager can then be used to uninstall the app.

We note that it was not necessary to enter a password to uninstall the software; this is an obvious security risk, as it means that a thief could simply uninstall the product, including the theft-protection component.

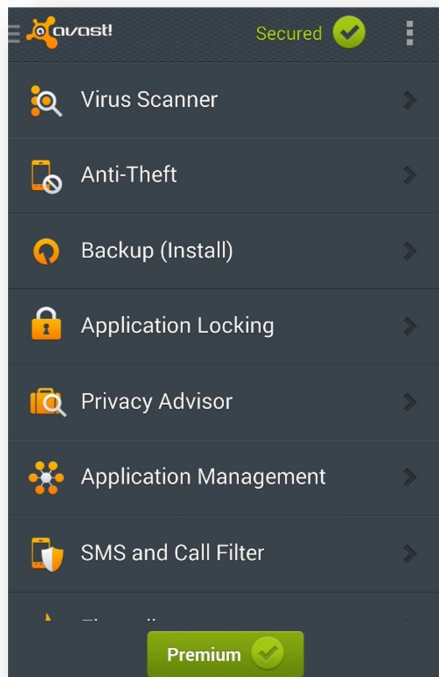
### Summary

AhnLab V3 Mobile provides the most important security functions for Android

smartphones. As well as the classic protection features such as theft protection, there are also innovative functions such as file encryption and network management. However, the product appears to have problems with the latest Android version; we found malfunctions with the anti-spam, lock screen and file encryption components.

## avast! Mobile Security

avast! Mobile Security is a free program. It is a comprehensive security product for mobile phones and tablets. The most important functions are antivirus, browser protection and theft protection.



### Installation

We downloaded avast! Mobile Security from the Google Play Store. The user is presented with an introductory tutorial that explains the most important functions. After this, avast! recommends scanning all installed applications. The user can skip this step if desired, however. If the scan is carried out, an update of the malware signatures is carried out.

### Starting the program

When the program is first started, the home screen is displayed, which indicates the extensive scope of the program. At the bottom edge of the screen, a "Go Premium" (paid-for version with extra features) button is shown.

Navigating the menus is largely an intuitive process.

### Virus Scanner

The Virus Scanner scans all installed applications for malware. The user can also choose to scan all files. Pressing and holding this checkbox displays a dialog, which can be used to select a particular folder for scanning. At the bottom of the screen, buttons are shown for configuring an automatic scan. Time of day as well as day of the week can be specified.

### Shield Control

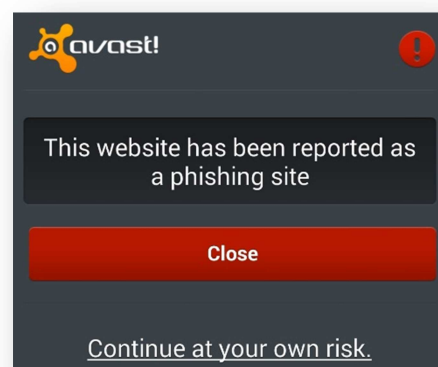
The various real-time protection features are termed "Shield" by avast!. The available shields can be found by swiping to the right. The following shields are available:

#### App Shield

The App Shield scans apps during installation and/or execution, depending on how it is configured.

#### Web Shield

This component protects the user against phishing sites and sites containing malware. The standard browser, Google Chrome, Amazon Silk and Boat Browser are all supported. In our quick test, the feature worked very well.



avast! also offers a spelling checker for URLs; this checks and corrects typos when website addresses are entered, to avoid "typo-squatting". In our test, however, we were not able to produce a situation in which avast! made a correction.

### Message Shield

This scans all incoming messages for phishing/malware URLs. This feature worked perfectly in our test. Messages with an unknown sender can also be blocked.

### File Shield

This scans for malicious behaviour during read or write processes. This also worked flawlessly in our test. The component is activated by default.

### Anti-Theft

The Anti-Theft component is a stand-alone app and has to be installed separately. This has the advantage that the app can be hidden. If the user has rooted the device, the theft protection can be installed in "hard-reset proof" mode. If this software is installed in this way, it will be available even after the device has been restored to factory settings.

A straightforward but fairly comprehensive setup procedure is required. The name and phone number of a trusted person, along with a PIN of between 4 and 6 characters, have to be entered. The user then has to log in with an email address or Facebook account, if the web interface is to be used. The telephone number [of the device being protected] also has to be entered.

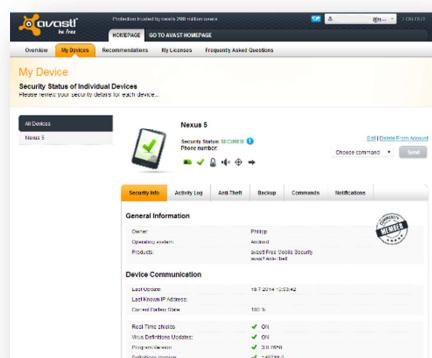
avast! offers a special binary format for Android 4.4 devices; this is necessary, as outgoing text messages could be read by a thief.

Activating the Anti-Theft component automatically switches on Stealth Mode, which completely hides the theft-protection function. If the PIN is dialed from the phone, the component becomes visible again.

A glaring yellow symbol signifies that there are problems with the configuration. For example, it will indicate that avast! has to be made a device administrator.

The Anti-Theft component can be controlled using the web interface (<http://my.avast.com>), or various text-message commands. As well as the classic

functions, such as lock, locate and wipe, avast! also offers redirection of calls, texts and call logs etc. An overview of all commands can be seen here: <http://www.avast.com/free-mobile-security#tab3> (click on "Control via SMS").



### Lock

#### Text-message command: "<Pin> LOCK"

When the command has been sent, the device is locked and a lock screen displayed. Honest finders are asked to report the find to avast!. The IMEI [International Mobile Equipment Identity] number, which is shown on the lock screen, has to be sent to [android@avast.com](mailto:android@avast.com). The text of the message can be edited. Additionally, a loud siren is sounded, and the message "This phone has been lost or stolen" played. This is only available in English. Entering the correct PIN will unlock the phone.

Overall, the lock feature worked well in our test. We were not able to get around the block and so could not access any personal data on the phone. We do however have some criticisms. We found that holding down the phone's power button activated aeroplane mode, whereby neither text messages nor the web interface would work. Additionally, the emergency call function is blocked when the phone is locked, which could be dangerous in some situations.

### Siren

#### Text-message command: "<PIN> SIREN ON"

This command sounds the same siren as for the lock function, but does not lock the



device. It is thus not a security feature, but helps the user to find a mislaid phone.

### Locate

**Text-message command:** "<PIN>  
**LOCATE<INTERVAL>**"

This command is used to determine the location of the phone. Once it has been sent, the sender receives a text message in reply, with co-ordinates, cell information and network provider. The optional parameter "interval", specified in number of minutes, can continually track the phone, even when the command is sent by text message. The user has the opportunity to use the web interface for this function, in which case the movement of the phone is displayed on a map. Naturally, this is much better suited to tracking the phone than a series of text messages.

The tracking can be stopped by sending the command "<PIN> LOCATE STOP"

### Wipe

**Text-message command:** "<PIN> WIPE"

This function deletes the user's personal data from the smartphone. avast! offers a number of different ways of doing this.

The conventional method does not reset the device to factory settings. In our test, personal data such as contacts, bookmarks, calendar entries and files was deleted, but not text messages or the Google account. Emails could thus be received and read just as before. On our alternative device with Android 4.1.2, the text messages were also deleted.

A thorough delete overwrites the SD card with junk files, which takes considerably longer, but prevents the personal data being recovered. However, in our test, this did not work. Using common freeware programs, we were able to recover a majority of the files.

If the program is made a device administrator, the wipe process can reset the phone to factory settings. This deletes text messages and the Google account too, but also removes the theft-protection software (unless the device has been rooted, please see above).

### SIM Change Lock

avast! includes a function that locks the device if the SIM card is changed by a thief. The user can configure the action to be taken in such an event; it is possible to lock the device and play an alarm siren.

### Backup

This function has to be installed separately, and enables personal data to be backed up. Google Drive is used as the backup location.

After activation, the user can decide which data should be backed up. Checkboxes are used to select from contacts, call logs, text messages, photos, audio and video files and apps. The option to back up only when connected via WiFi is sensible. It is also possible to specify that backup should only take place if the battery life is above a certain level.

Triggers can be set to start the backup process; for example, every time the device is started or every time the charger is connected. Additionally, the backup can be run on a schedule, with day of the week and time of day specified.

The backed-up files can be seen in the Google Drive web interface. avast! state that contacts, texts and call logs are saved on avast! servers in addition to Google Drive.

### Application Locking

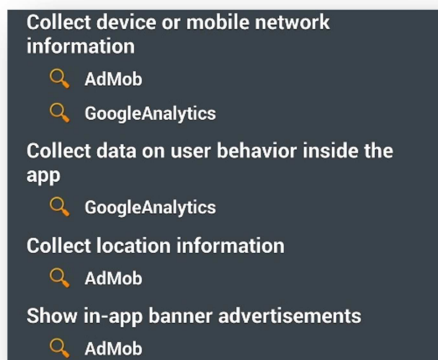
This function allows specific apps to be password protected. Any and all installed apps can be protected in this way. avast! recommend using [the app block](#) to protect the Google Play store and settings as well, [because otherwise an unauthorised person could bypass the feature.](#)

### Privacy Advisor

The Privacy Advisor categorises apps that have privileges such as access to messages, location or contacts. This provides the user with an overview of possible privacy violations. Tapping one of the seven categories shows the apps that have the relevant permissions. If the user then taps one of the apps shown, detailed information

and a button to stop the app immediately are shown.

Additionally to displaying the permissions, avast! also provides an Ad-Detector, which shows all the advertising networks that are integrated into an app. Google Analytics, AdMob, etc. are thus displayed. The permissions of the ad networks are also shown. For example, the user can see if an ad network has the right to locate the device, or display ads in full-screen mode, or show advertising banners.

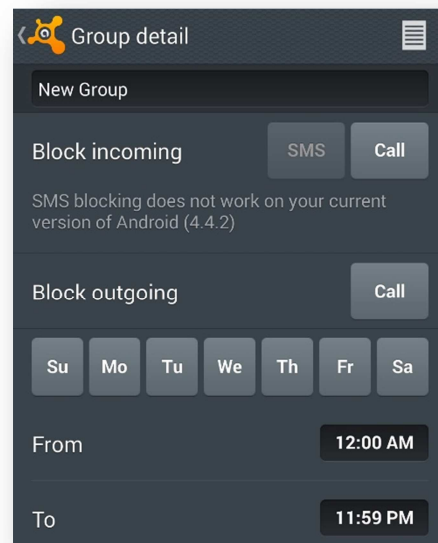


### Application Management

The Application Manager makes it possible to check installed and running apps for CPU load, RAM, storage space etc., and to shut them down.

### SMS and Call Filter

To prevent the user being bothered by unwanted calls and text messages, avast! provides the SMS and Call Filter. This allows the user to create groups of numbers that should be blocked. The times at which calls/texts should be blocked can also be specified.



Numbers can be taken from the address book and call logs, and anonymous or unknown callers can also be specified. The feature relies on the blacklisting principle. Thus, all callers are allowed that do not belong to one of the blocked groups.

avast! makes clear to the user that the text-blocking feature is not compatible with the current Android version. However, on our alternative test device, which runs Android 4.1.2, the feature worked as expected.

### Firewall

The firewall is inactive and cannot be used unless the device has been rooted. This is in accordance with restrictions by the OS on non-rooted devices. As the scenario for our test assumes an average user, whose device has not been rooted, we were not able to test this feature.

### Network Meter

This component lists the data volume used by installed apps. This can be broken down into WiFi, 3G, Roaming and Total. Tapping an app allows its data usage to be displayed by date (today/month/year).

### Updates

Updates are carried out automatically. The network(s) to be used for updates can be



selected (WiFi, 3G, Roaming). Updates can also be run manually.

### Help

There is no help function within the app. This could be problematic, due to the scope of functionality and configuration options in the app. A user guide (34 pages) and FAQ can be found on the avast! website.

### Deinstallation

The uninstallation of avast! can be carried out without entering a password. However, the theft-protection functionality remains active, as it is contained within a separate app.

### Licence

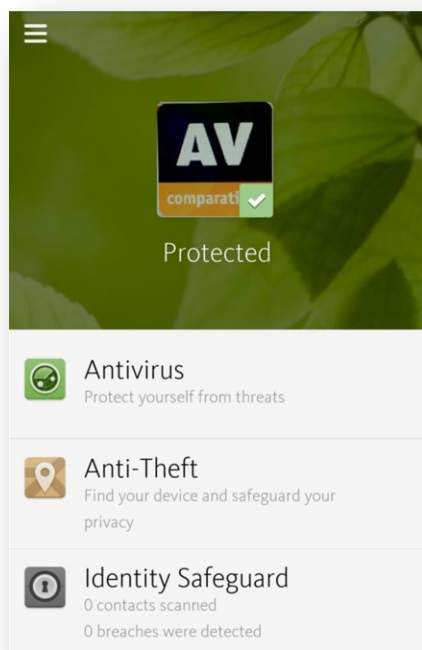
avast! Mobile Security is available as a free app with reduced functionality. Premium functions such as App Locking, Ad Detector, some anti-theft features, and the backup function can be obtained by purchasing a Premium Plan, which is available for €1.99 a month or €14.99 a year.

### Summary

avast! Mobile Security has a wide range of features with innovative functionality. We particularly liked the wide range of configuration options and remote commands, which provide the user with a comprehensive remote control function. The Backup, App Locker and Privacy Scan features, which were promised last year, have now been implemented and complete the program's functionality.

## Avira Antivirus Security

Avira's Antivirus Security is a well-designed security product containing important security features such as a malware scanner, theft protection and blacklist. The product is completed by innovative features such as Identity Safeguard.



## Installation

Avira Antivirus Security was downloaded without charge from the Google Play Store. The first step is to create a new Avira account or log in with an existing one. Creating an account requires an email address and a password of at least 5 characters. Avira also recommends storing a photo, along with first and last names, in order to make it easier to find the device if lost. Once the user is logged in, the antivirus component is updated and a scan is performed.

## Starting the program

When the program is started, a well-designed home screen is displayed. In the middle of the upper part of the screen, a picture of the user is shown, along with a message stating that the user needs to take action. This is because the anti-theft component has not yet been set up.

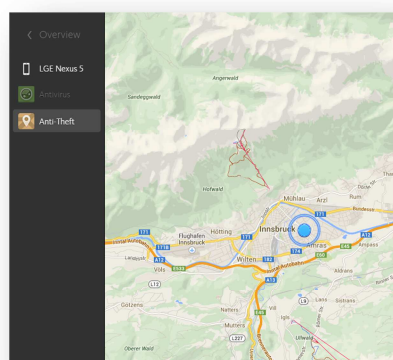
The home page also lists the most important functions. A context menu, which can be opened by swiping from the left, allows the profile to be edited, settings to be changed, and the help function to be started.

## Antivirus

The Antivirus component can be found in the menu entry of the same name. It allows installed apps and files to be scanned for malware. Avira shows statistics regarding the number of checked apps and files and the date of the last scan. At the end of the list, the version of the currently used virus definitions is shown, along with the date of the next automatic update. A manual update is not possible. The user can use the settings to change the categories of threats to be detected. Adware is selected by default, and PUA (Potentially Unwanted Applications) can be selected in addition.

## Anti-Theft

Avira's theft-protection component is controlled by a well-designed web interface (<http://my.avira.com>). Text-message commands are not available. The web interface allows multiple devices to be managed from one account.



The home page of the software displays an alert that the program is not registered as a device administrator. A message box explains that this must be configured to allow remote wipe by resetting the device to factory defaults. It is also noted that device administrator privileges are also required for

the remote-lock function on some tablet PCs. Tapping the "Activate" button makes Avira Antivirus Security a device administrator, whereby the status shown on the product's home page is changed to "Protected".

#### **Play Sound**

The alarm function sounds a shrill siren for 20 seconds. The device is not locked, as the purpose of the function is to allow the user to find the smartphone again when it has been mislaid, rather than to scare off a thief.

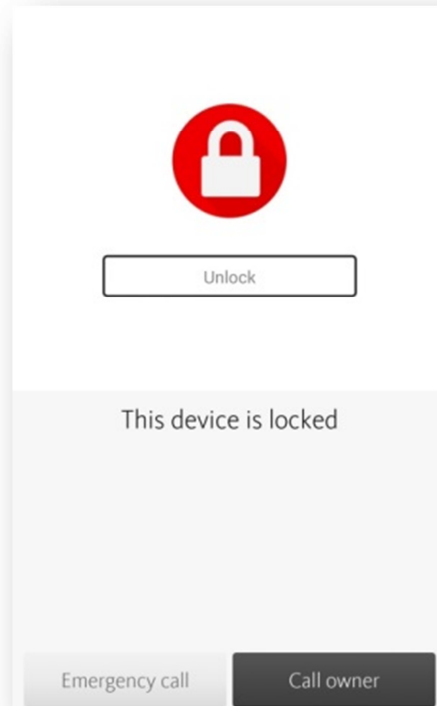
#### **Find Device**

This feature finds the device and displays its location on Google Maps. The address of the location is also shown. If multiple devices have been connected with the same account, these can all be seen together on the same map. The process of locating the phone has to be started manually each time it is needed, a continuous tracking facility is not included.

#### **Lock Device**

This feature uses a lock screen to prevent unauthorised access to the phone. Via the web interface, the user can put in a four-digit numerical PIN which can then be entered on the phone to unlock it. Alternatively, the web interface can be used to remove the lock. A user-defined text can be displayed on the lock screen, which could provide an honest finder with the owner's contact details. We find this sensible. Additionally, a telephone number can be provided which will be called if the finder taps the button marked "Call Owner"; the number is not displayed on the screen.

To unlock the screen, the previously defined PIN has to be entered. After three incorrect entries, the PIN entry is blocked, and the device can only be unlocked using the web interface.



We found the lock function to be very well implemented. It was not possible to bypass the lock or access the phone any other way. An emergency call is always possible.

#### **Wipe data from device**

This function allows data on the device to be deleted remotely. The web interface allows the user to decide which data to wipe. Checkboxes can be used to select data on the SD card and/or SIM card, as well as resetting the device to factory settings. If the latter operation is carried out, the anti-theft features will not be available any more. However, it is the only way to remove all user data such as contacts and calendar entries.

We tested the deletion of data on an external SD card. Whilst this functioned as expected, we were able to recover the deleted files using a common freeware program.

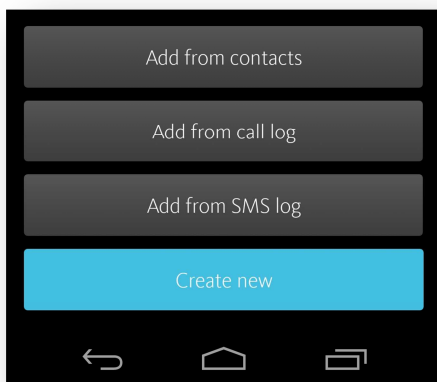
#### **Identity Safeguard**

This feature warns the user in the event that his or her email address has been affected by a major data leak. Adobe (for example) has been affected by data breaches that have allowed a large number of user credentials to come into the public sphere. Avira checks

whether the user's email address, or an email address in the Contacts list, has been involved in such a data breach against a database of more than 160 million breached email addresses.

### Blacklist

The blacklist allows specific phone numbers to be barred from calling the user or sending text messages. Numbers to be blacklisted can be imported from Contacts, call lists and text-message logs; they can also be entered manually. For each individual entry in the blacklist, it can be specified whether just calls, just text messages, or both should be blocked.



Before the feature is first used, a warning is shown that the software may encounter some problems with specific models of LG mobile phones, meaning that the call-blocking feature will not work. Text-message blocking is not affected.

In our test, exactly the opposite occurred. Calls were blocked as expected, but text messages were allowed through despite the sender's number being blocked. This state of affairs is actually described in Avira's description of the software in the Google Play Store, which notes that the function does not work with Android 4.4.2, our main test version. Text messages were blocked successfully on our alternative test device with an earlier version of Android.

### Upgrade

An update can be purchased from Avira that adds a "Secure Browsing" component. This protects the user against malicious content whilst surfing the web. Additionally the upgrade provides comprehensive customer support and hourly updating virus definition files.

### Updates

Updates are carried out automatically. The interval is fixed and cannot be changed. In the free version of the software, an update is run every day, in the premium version every hour. A manual update is not possible.

### Help

The Help link in Avira's menu leads to "Avira Answers". This website is very inconvenient to use with a mobile phone. Avira Answers is a community forum that allows users to discuss common questions.

### Deinstallation

Avira has to be removed from the list of Device Administrators before it can be uninstalled. A wizard is provided that takes care of all necessary steps. The user is asked for his/her reasons for uninstalling the software, though this step can be skipped. Deinstallation does not require a password to be entered. This makes it possible for a thief to uninstall the software if the owner has not yet remotely locked it.

### Licence

Avira Antivirus Security is available free from the Google Play Store. The Premium version, which includes the Safe Browsing feature, hourly updates and extended support, costs €7.95 per year.

### Summary

Avira's Antivirus Security is a well-designed security product for Android smartphones. The theft protection can be controlled using an equally well-engineered web interface. Innovative functions such as Identity Safeguard complete the product. Avira

appears to be aiming for quality rather than quantity. The scope of functionality is relatively limited in comparison with other products, but the components that are included have been implemented very well. We would however like to see password protection for the uninstaller.

## Baidu Mobile Security

Baidu Mobile Security is a free security product, which offers many functions including mobile tuning, app management, protection against nuisance calls and spam texts, antivirus and mobile payment protection.



### Installation

We downloaded Baidu Mobile Security from the official Baidu download site without any difficulty. The installation was very simple.

### Starting the program

When the program is started for the first time, the Baidu mobile payment protection is recommended to the user.

The end-user licence and the option to send app feedback is marked as accepted by default. The user can try the payment protection or go to the main menu by tapping on the option in the upper right-hand corner.



On home screen, all functions can be accessed with a single tap:

### Health check-up

In the center of the window, a circular display shows the current "health" of the mobile device. The check-up function frees memory, ends processes and removes trash files. The feature recommends activating the safe-payment function and upgrading already installed apps, and points out that a full scan has not been carried out. The full scan reports a promotional app published by the Aochan supermarket in China as malicious.

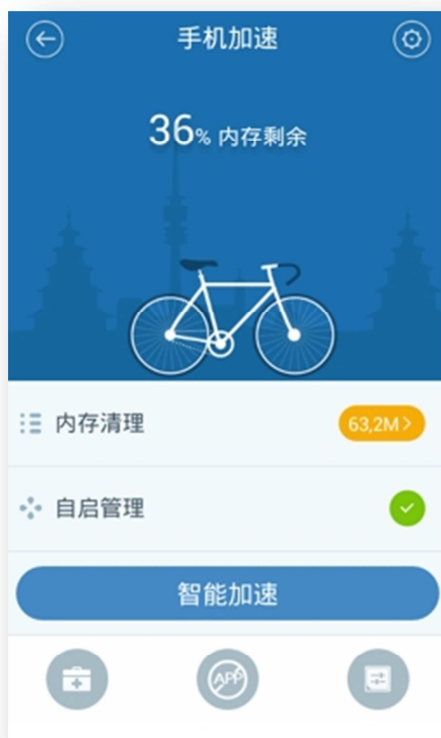
During the check-up, the installation of the Baidu App store is recommended "for safe app downloads."

### Mobile Speedup

After the check-up, the mobile phone speedup still found further possibilities to speed up our test device. According to the app, we freed 500 MB of memory with the "smart speedup" function.



The function offers “deep speed up” which first has to monitor the apps on the test device for a longer period. Apps cannot be frozen or the CPU speed changed without first rooting the device.



### Trash removal

After the check-up and the mobile speed-up, the trash removal function still found 45 MB of trash on the test device. The deep removal function even found 92.5 MB of trash.

### Mobile fee protection & data volume monitor

The current Baidu app offers a whole set of functions to protect the user from high mobile-phone fees. On the tab “Protection against waste of mobile fees” the user can see the mobile phone balance and the data volume that has already been used. The user can scan a device for apps that cause high phone fees, see which apps have caused unusual data traffic, cancel mobile value-added services and check the inbox for fraudulent text messages. On the test device with a China Unicom prepaid SIM card, the check for mobile value-added services did not

work properly. An in-app text explained that Unicom users had to contact the mobile operator to check manually for value-added services they have ordered.



### Data traffic monitor

This component monitors the mobile data traffic of the user. The app can synchronize the data periodically with the billing system of the mobile network operator. The user can buy additional volume within the app. The app reminds the user that surfing the Internet while travelling abroad is not covered by the monthly data package.

### Disturbance blocker

Spam texts and nuisance phone calls are still serious problems for Chinese users. In our test, the app correctly blocked spam texts. Unfortunately, none of the mobile and fixed-line phone numbers that were used at the time of the review for unsolicited sales calls was identified in our test.

### “Security” Tools

A large variety of other security and non-security related tools can be downloaded and installed via this tab, such as flashlight

(torch), WIFI radar, energy saver, one-click root, games speed-up and many more.

### Secure Payment

Secure payment has been given its own tab. Users can check their transaction records. On this tab, the official download link for many popular banking apps is provided. Apps such as the taxi app Kuaidi Taxi and the Alipay wallet can run in a "secure environment." The safety of the WIFI network can be checked and text messages relating to online payments can be "protected."

### Further functions

In the lower corner of the main tab, the user can finally find the home of the AV scan function, next to a function to root the device, another memory cleaner, an app uninstaller, an adware scanner, a privacy scanner and a safe input form for the Baidu search engine. The AD scanner reported a privacy risk in Rozio's game Amazing Alex, which can obtain the number of the mobile device, and recommended deinstallation. No other threats were reported.

### AV Scanner

Baidu offers two scanning options, "Complete system scan" and "Quick scan". The malware definitions are updated automatically. By default, the cloud scan is active and all app installations are checked.

The same Aochan app that had just been declared to be safe by the Baidu AD scan was reported to be malicious by the Baidu AV scan, which encouraged us to uninstall the app immediately.

### The Baidu spaceship

After installation of the Baidu app, our test device had a tiny circular object at one side of the mobile desktop. Dragging this object to middle of the screen starts a plane, which thunders Star-Wars-like over the screen riding a laser beam. This action performs a quick clean-up of the device.

### Deinstallation

There is no uninstallation wizard. No password is required to uninstall the product. Because there is no anti-theft component this might not be a problem, as uninstallation protection is not required.

### Licence

Baidu Mobile Manager is free.

### Summary

Baidu Mobile Security is still an easy-to-use product with important security features like nuisance protection and safe payment. The accuracy of the nuisance-call detection should be improved, however.

Any danger detected by any module of a security product should be clearly visible throughout the app: Users with no technical background might believe that as long as the health score of the mobile device (displayed prominently on the main tab) is high, no other checks are necessary.

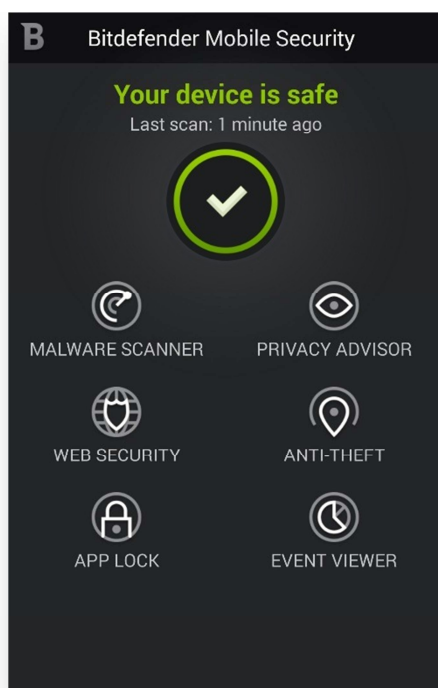
Health score	92
Ad scanner	No risk
Av scanner	VIRUS

Furthermore, we still recommend adding theft protection, as the danger of unauthorized access to private information on stolen or misplaced mobile devices should not be underestimated.



## Bitdefender Mobile Security

Bitdefender Mobile Security is available as a 14-day test version. After the test period, the user has the option to purchase a licence in order to continue using the software. Bitdefender's mobile product combines a cloud-based malware scanner with privacy capabilities, web protection and an anti-theft feature. The latter can be controlled by text messages or a web interface that lets you lock, track, and wipe your Android from any Internet-connected device. The latest version of the app also features an Android Wear extension allowing Android users to make better use of their Smartwatch by turning it into an anti-theft tool and a perfect phone locator.



### Installation

Bitdefender was downloaded free from the Google Play Store. The first step is to accept the licence agreement. The user can then opt out of sending anonymous statistics to Bitdefender.

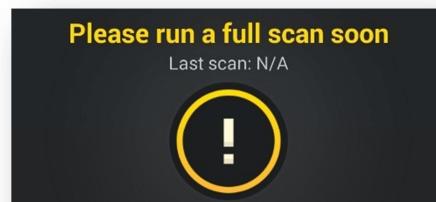
The device then has to be given a name to identify it in the web interface. Next, a user account has to be associated with the device. A new Bitdefender account can be created, or an existing Google account can be used.

Finally, the product has to be licensed. There are options to try the product for 14 days, buy a licence, or enter an existing licence key.

### Starting the program

When the installation has completed, the user is taken to the program's home page. A prompt to complete a scan (in yellow), and an orange banner reminding that a 14-day test version is being used, catch the user's eye.

When a malware scan has been carried out, the status display will show one of three possible states. Green indicates that all is well, while yellow or red indicate smaller or larger security risks requiring the user's intervention.



Bitdefender does not report on the status of updates. This is because the malware definitions are not saved locally but reached via a connection to Bitdefender's cloud service.

### Malware scanner

The malware scanner allows the user to scan installed apps for malicious programs. As an option, the phone's memory can also be included in the scan. An automatic scan of the installed apps runs during the installation process.

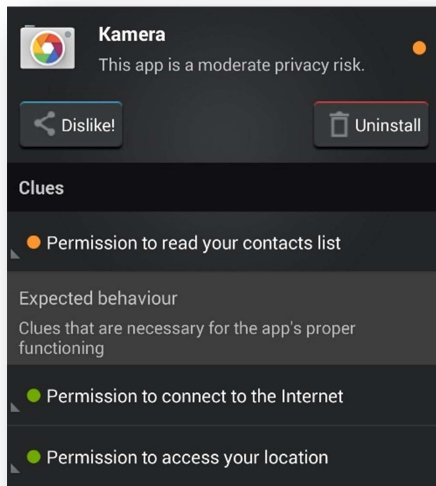
The malware scanner requires an Internet connection, due to the cloud being used for malware detection.

### Privacy Advisor

The Privacy Advisor analyses installed apps to see if they record private user data and thus threaten the user's private sphere. To avoid overloading the user with details, Bitdefender provides a score between 1 and 100, representing the overall security situation.

The lower the score, the greater the number of apps with dubious privileges that have been detected.

Additionally, all installed apps are displayed in a list. Tapping an app's entry in the list displays all its privileges.



This has been well implemented, in our opinion. App privileges are divided into "Expected behaviour" and "Clues". This allows even inexperienced users to evaluate the information and decide for themselves whether there is any evidence of spying by the app. In this view, the app can be uninstalled directly.

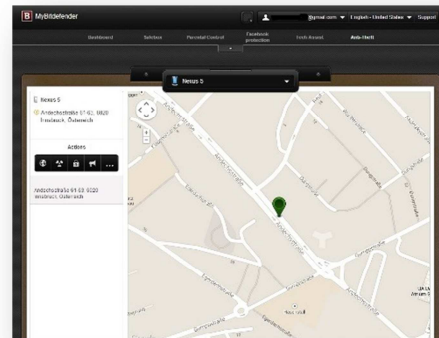
### Web Security

Web Security protects the user against common threats whilst surfing the Internet. Bitdefender states that the product protects against phishing, other types of fraud and malware.

### Anti-Theft

Bitdefender's theft protection features can be controlled by an elegant web interface (<http://my.bitdefender.com>). The feature is not activated by default, but can be enabled quickly. The device has to be made a device administrator in order to obtain the necessary privileges for delete/lock commands. Bitdefender points out that the device administrator status has to be deactivated before uninstalling the product. To complete

the process, a PIN of between four and eight numerical characters has to be entered. Additionally, details of a trusted person have to be entered. He or she will be contacted in the event that the SIM card is swapped, and the phone number will be the only one from which the wipe command can be sent.



### Locate

**Text-message command: *BD-<PIN> LOCATE***

The Locate function finds the position of a lost or stolen device. The web interface displays the location of the phone in Google Maps. Continuously locating the phone is not possible.

If text messages are used to control the software, the sender will receive a text in return that contains a link to the phone's current location in Google Maps.

### Scream

**Text-message command: *BD-<PIN> SCREAM***

The Scream function sounds a shrill siren. The device is not locked. The function thus serves to help the user find the phone when mislaid, rather than scaring off a thief.

### Lock

**Text-message command: *BD-<PIN> LOCK***

This command locks the device and protects against unauthorized access. Bitdefender uses the lock screen that is built into Android. This does not allow Bitdefender's own logo or messages to be shown, but has no security-related issues. It cannot be bypassed, and an emergency call can always be made.

If the command is sent by text message, the previously entered four to eight-digit Anti-Theft PIN can be used. If the web interface is used, a four-digit PIN can be assigned.

### Wipe

#### **Text-message command: BD-<PIN> WIPE**

This command resets the device to factory settings and deletes all the data on it. The Wipe command can only be sent by text from the number of the previously registered trusted person.

The function worked well in our test, with one exception: no data was deleted from the external SD card, which was also the case last year.

### CallMe

#### **Text-message command: BD-<PIN> CALLME**

This command can only be given using a text message. When the command has been received, the phone number used to send the text will be called, and the phone's loudspeaker will be activated. This makes it possible to contact the finder of the phone, and (if this person is honest) to arrange for it to be returned.

### Help

#### **Text-message command: BD-<PIN> HELP**

An under-appreciated but nonetheless very useful command is Help. Sending this to the lost or stolen phone produces a text message in reply that contains a list of all other possible commands. This makes sense if the phone's owner cannot remember all the possible commands; he or she only has to remember one.

### SIM Change

If the phone's SIM card is changed, e.g. by a thief, a text is sent to the previously registered trusted person. This person should then inform the owner; there is then no point in trying to use text-message commands to lock or locate the phone.

However, the feature did not work in our tests. We replicated the scenario exactly, but no text message was sent, and there was no

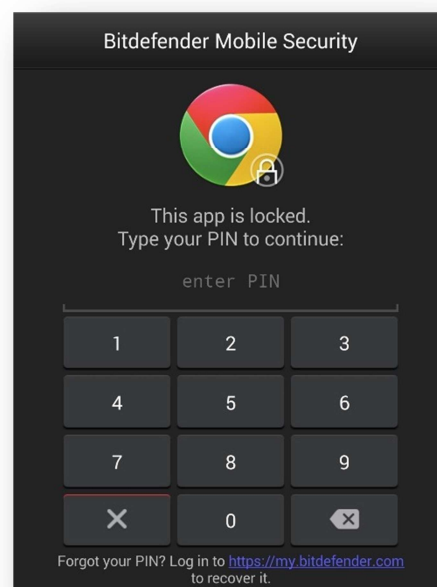
evidence of any other activity being carried out by the security product. However, on the alternative test device with Android 4.1.2, the feature worked perfectly.

### Upload Location

This feature uploads your last known location to <http://my.bitdefender.com> before the phone's battery runs out.

### App-Lock

App-Lock is a new feature in Bitdefender's suite. It password protects individual installed apps. The user can specify which apps require a password. For example, opening the Gallery can be made demand the entry of a PIN. This could be used e.g. to prevent children from using particular functions of the phone.



### Updates

As Bitdefender Mobile Security does not include an offline scanner, but always uses the Bitdefender Cloud service to check for malware, and update function is not required.

### Help

There is no help function as such within the program. Each function does however have its own short explanatory tip.

## Deinstallation

There is no uninstall wizard. The PIN has to be entered before the software can be removed, thus preventing a thief from removing the theft protection.

## Licence

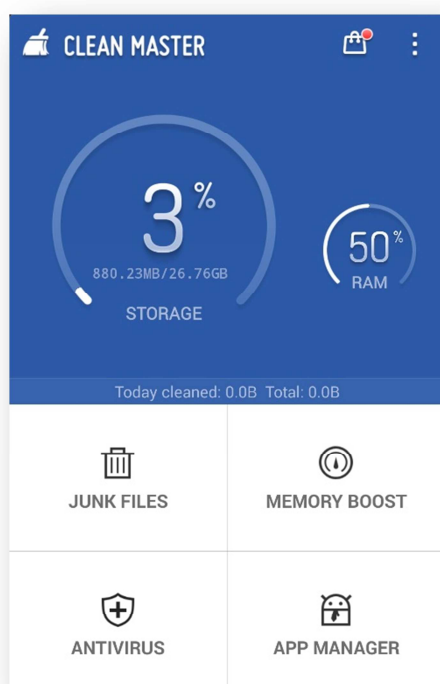
Bitdefender Mobile Security PREMIUM can be tested for 14 days without charge. After the trial period, a licence has to be purchased to continue the use of the software. This costs €9.95 for a year or €0.99 per month using in-app purchase.

## Summary

Since last year's review, Bitdefender Mobile Security has been graphically reworked and extended to include the App Lock function. The features are well thought-out and largely worked very well. Only the SIM Change function did not work with the latest Android version.

## CheetahMobile Clean Master

CheetahMobile Clean Master is a security product that specialises digital cleaning of the mobile phone. The components are Antivirus, Junk Removal, and Memory Boost. There is no theft protection.



### Installation

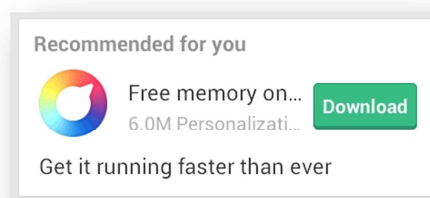
CheetahMobile Clean Master was installed from the Google Play Store. No further configuration is required after the installation; the user is taken to the program's start screen.

### Starting the program

When the program is started, the start screen displays the current storage usage and RAM usage. Statistics for the number of bytes cleaned up in the current day are also shown. As the program has only just been installed, the display shows zero bytes. Tapping on the Storage icon shows a detailed list of the storage usage; there is a parallel function for the RAM icon.

### Junk Files

This function finds unnecessary files, e.g. cache files, in the local file system. The program offers to delete these files and thus clean up the system. Our device, which had only been used for a few simple tests, had collected 578 MB of junk files, according to Clean Master. Amongst the files to be deleted were some obsolete APK files, files in phone storage that were no longer needed, and cache files. When the cleaning process has been carried out, the results are displayed (575 MB in our case); suggestions for additional apps are displayed:

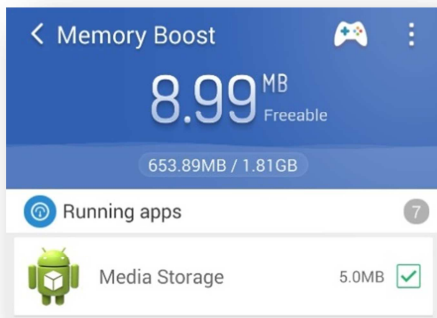


After using the device briefly, without starting any other apps, a further 177 MB of storage space was freed. The manufacturers tell us that this is because most apps have background services, which periodically generate unnecessary files (junk files).

Deleting junk files can be set to run automatically. The user can choose an interval between one and fifteen days. It is also possible to filter by file type. Thus JPG files, for example, could be excluded from the cleaning process.

### Memory Boost

The memory boost function cleans unnecessary processes related to running applications.

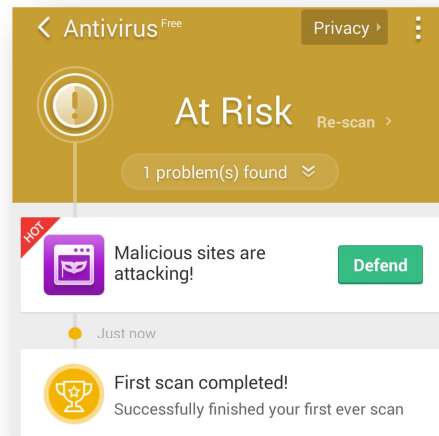


In our test, apps such as the clock and Media Storage were shown. Additionally, some apps, such as Hangouts, are shown, but with the recommendation to keep them running. In our test, 9 MB of data were removed from the RAM.

### Antivirus

The antivirus component of the product examines the device for potential security problems. CheetahMobile do not consider simply scanning the file system to be sufficient. In our test, it was pointed out that the browser history (Chrome) could be deleted. Additionally, real-time protection is provided.

At the top of the screen, a button marked "Privacy" is shown. This button can be used to delete any data relating to the way the device is used. An example would be the search history in the Google Play Store. A simple tap on "Clean" removes such entries from the device. As well as the automatic cleaning, there is a manual cleaning function. Clean Master leads the user to relevant apps, from which the cache and other data can be deleted.

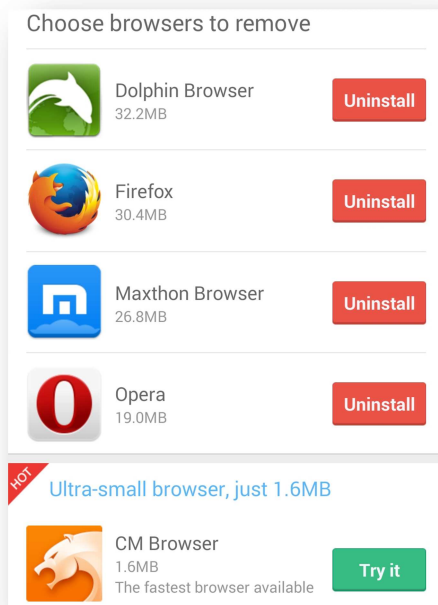


In our test, when the virus scan was completed, a notice was shown stating that "Malicious sites are attacking!" along with a "Defend" button. Tapping this button only took us to the Google Play Store, from where CheetahMobile's own browser could be installed. We found the choice of words to be unnecessarily alarming, and feel a more neutral way of pointing out the safe browser would be appropriate. We repeated the test a number of times, also using a second device; on one occasion the same warning was shown, on others there was a different message.

### App Manager

The App Manager displays a list of installed apps. In our case, it showed that four browsers were installed, taking up a total of 108 MB of storage space. Individual apps can be uninstalled directly from this menu. A suggestion is made to uninstall the current browsers (Opera, Dolphin, Maxthon and Firefox) to recover space, while the CM browser is promoted:





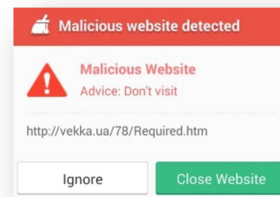
At the end of the list of installed apps is a further list of recommended apps (approximately 100). Swiping to the right changes the user interface to "Picks", where particularly popular apps are listed.

Another page of the program shows APK files that have been found on the file system. This is oriented towards removing the files, although it would be possible to execute a file and thus install its app.

A further function of the app manager is to move other apps from the internal storage to an external SD card. This could be useful if the internal storage were limited, but plenty of space is available on an SD card. However, the function turned out to be incompatible with both of our test devices.

### Safe Browsing

Clean Master has integrated a safe browsing feature. This protects the user against fraudulent and risky websites whilst surfing the net.



In our quick test, this worked very well.

### Updates

We were not able to find any information regarding updates. Clicking the Update button took us to the Google Play Store.

### Help

An FAQ with 42 items is provided. Whilst this clarifies some issues, we feel that a more conventional help service would be more helpful.

### Deinstallation

The product can be uninstalled using Android's built-in App Manager. It is not necessary to enter a password. This is perfectly acceptable, as the software does not include theft protection.

### Licence

CheetahMobile Clean Master is available free of charge with full functionality.

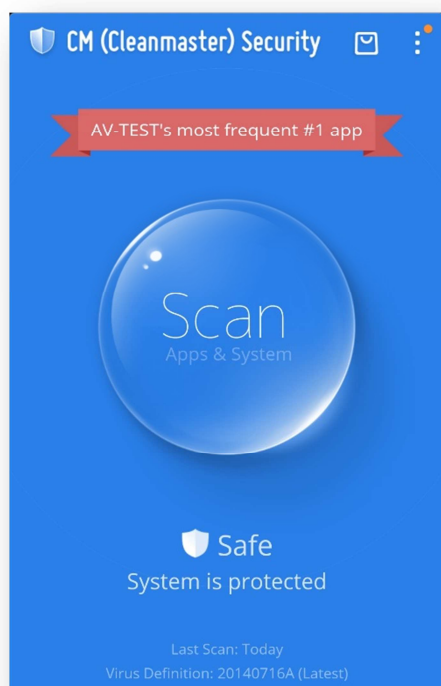
### Summary

CheetahMobile Clean Master adopts a different approach from most of the security products in this test. There is no theft protection, the focus instead being on digitally cleaning the device. The cleanup function allegedly freed up astonishing amounts of storage.

We regard the risk of loss or theft as being ever-present. Although the antivirus and cleaning components work well, we feel that the product would be made complete by a theft-protection module. Users should be aware that the software may suggest removing some existing programs from other manufacturers, and replacing them with CM products which are supposedly smaller or faster.

## CheetahMobile CM Security

CM Security is available free of charge, and offers useful functions such as antivirus and theft protection. Nuisance calls can also be blocked using the integrated call filter.



### Installation

CM Security was installed from the Google Play Store. The installation was unproblematic, and once started it required no further user interaction.

### Starting the program

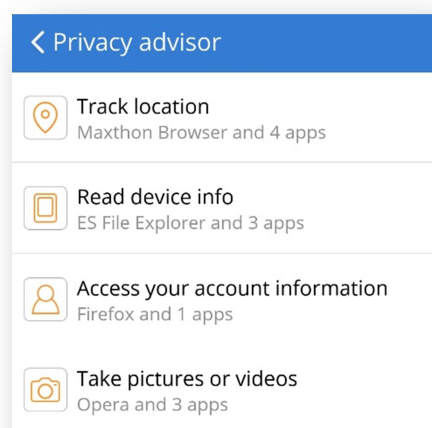
When the program is first started, a yellow status display is shown, along with a message that a security scan has not yet been carried out. When a scan has been carried out, another warning is shown by Cheetah Mobile, stating that Safe Browsing has not been activated. When this too has been carried out, the status display changes to blue, with the text "System is protected".

### Antivirus

A virus scan can be run directly from the app's start screen. This scans the system and installed apps. The SD card and integrated

storage can be scanned by selecting "Scan SD Card" from the context menu.

When the scan has finished, results are displayed - these include security recommendations. For example, CheetahMobile recommends installing "Safe Browsing". This is a link to the manufacturer's own "CM Browser" in the Google Play Store".



A Privacy Advisor can be found amongst the recommendations. This lists possible privacy breaches, shown in four categories. In our test, the categories "Location", "Device Info", "Access Account Information" and "Creating photos and videos" were shown. Tapping one of the categories displays the apps with the related permissions. If one of the apps in the list is then itself tapped, details are displayed. In our opinion, this process leaves room for improvement. Only the privileges in the current category are shown. If the app has been assigned to multiple categories, the user has to go through all the categories one by one, as no overview is provided. This makes it difficult to decide if an app really represents a security risk.

The user can rate the app as "Trusted" or "Questionable". This evaluation is apparently sent to CheetahMobile.

CM Security also indicates that real-time protection, safe browsing and automatic updates are all activated.

The SD card and integrated storage can be scanned by selecting "Scan SD Card" from the context menu.



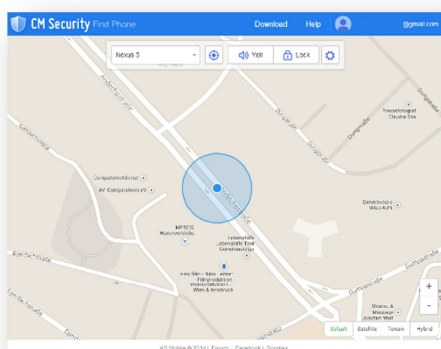
Automatic scans can be configured in the settings. They can be set to run on a daily weekly or monthly basis.

### Clean Up Junk

This component is not included in the default configuration, and is installed separately the first time the user attempts to access it. This takes the user to the "Clean Master" app in the Google Play Store, which is reviewed separately in this report. Please see the relevant section for details.

### Find Phone

This menu item is for the theft-protection component. When this is run for the first time, the user has to add an account. This has to be a Google account. An unlock pattern then has to be entered, which will be used to unlock the screen. This has to contain at least four points.



### Locate

This function locates the device and shows its position in Google Maps. When the web interface is opened, the device is automatically located.

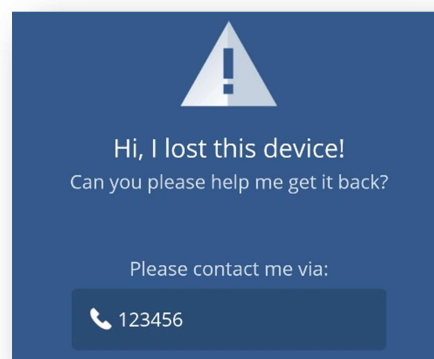
### Yell

This command sounds a shrill siren for 60 seconds, whereby the device is not locked. The function can be useful for locating a mislaid phone.

### Lock

This command locks the device, requiring the previously entered pattern to unlock it. The function works very well, we were unable to

bypass the lock. We also liked the fact that a telephone number and email address can both be displayed on the lock screen, thus helping an honest finder to return the device.



The lock screen is not perfect, however. It is not possible to make an emergency call, which would be dangerous in an emergency. We were also able to open the Android Notification Center, from which the device can be put into aeroplane mode. In this state, neither text messages nor the web interface can contact the theft-protection software, rendering it effectively useless.

A more positive point is the complete locking of the screen for a minute after multiple failed unlock attempts. This makes brute-force attacks more difficult.

### Wipe

The Wipe function deletes personal information from the phone, making it inaccessible by third parties. The first time we tried to test this, the relevant button was not shown in the web interface, and so we were unable to proceed. The manufacturer informed us that the feature was not available in our area (Austria), although the app itself showed the status as "enabled". CheetahMobile then made the function available, and so we were able to try it out.

The function does not reset the device to factory settings, which has the advantage that the theft protection remains active, and the device can be located. Unfortunately, CheetahMobile has not included some types of personal data in the wipe feature. Mails,

calendar entries, browser history and bookmarks were still accessible after the wipe. On our Nexus test device, text messages were not deleted, although the manufacturer warns the user of this in the web interface. This is a known issue with Android 4.4. On our alternative Samsung test device with Android 4.1.2, the text messages were deleted as expected.

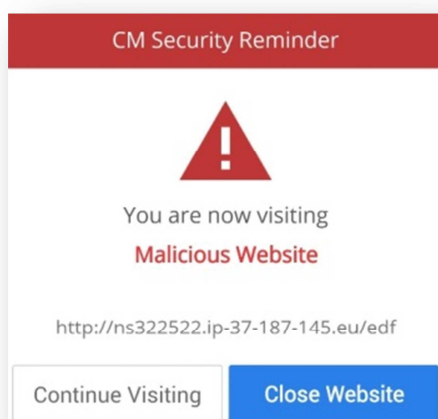
The wipe function deleted files on the SD card of our Samsung Galaxy, although it was easy to recover them with our usual freeware tool. We see room for improvement with the Wipe function.

### **SIM Alert**

This function sends an email to the user if the SIM card has been changed. This worked very reliably in our test. The device is not locked, however.

### **Safe Browsing**

The safe browsing function is almost invisible, being just a button in the app's settings. We could not find out exactly which threats the feature is supposed to protect against. However, it worked perfectly in our quick test with phishing sites.



### **Call Blocking**

This component can block calls from particular numbers. It works on the blacklisting principle, i.e. the user has to enter the numbers to be blocked. These can be entered

manually, or imported from the contacts and/or call logs.

The feature worked well in our tests. Care is needed when entering phone numbers manually, however. Calls are only blocked if the number is entered with the relevant international code, but without the leading zeros (e.g. 436991234.. for a number in Austria).

### **Updates**

Updates can be carried manually by tapping the appropriate button. Automatic updates are also offered; however, no information about the frequency is provided.

### **Help**

We were not able to find any type of help function.

### **Deinstallation**

The product can be uninstalled using Android's own App Manager. It is not necessary to enter a password. This means that a thief could simply remove the theft-protection software.

### **Licence**

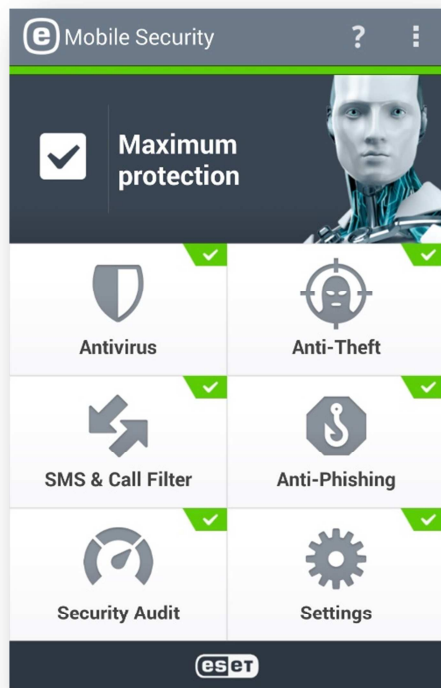
CheetahMobile is provided free of charge.

### **Summary**

CM Security is a mature security product. The theft protection worked effectively and reliably. We liked the fact that almost all the functions are essentially well implemented. However, we feel that the Wipe feature needs to be improved.

## ESET Mobile Security

ESET's Mobile Security is a security app that provides antivirus and anti-theft components. The Premium version also includes text-message and call filtering, phishing protection, system audit, extended theft-protection and a SIM guard. This year's version has been enhanced with a web interface.



### Installation

ESET Mobile Security was installed from the Google Play Store. To start off with, the licence agreement has to be accepted. In the next stage, the user can agree to send anonymous app-usage data to ESET. This option is deactivated as standard. After this comes the option of joining ESET's Live Grid, which is activated by default. This is a type of early-warning system that uses data collected from all participating users. The next step is to decide whether ESET Mobile Security should detect PUAs (potentially unwanted applications). Finally, the licence is checked, and a message is displayed to inform us that ESET is starting its first scan.

### Starting the program

After the initial configuration, the user is taken to a clearly laid-out start screen. This provides access to the individual components of the suite. Active components show a green tick (checkmark), inactive components have a grey button. The Premium version of the software can be tested for 30 days free of charge; an email address has to be provided. In the upper part of the screen, a tick (checkmark) and the text "Maximum Protection" are displayed. This might give a false impression, as the antivirus is the only active component, all the others are inactive.

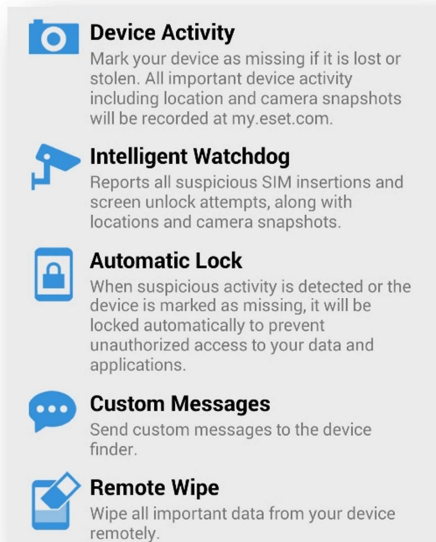
### Antivirus

The antivirus component lets the user scan the system for malware. The depth of the scan can be configured. As well as manual scans, automatic scans can be defined. There is also an "On-Charger Scan", which is triggered by the connection of the device's charger. We find this sensible. It is also possible to see the quarantine, list of ignored threats, scan logs and update history. Malware definitions can be updated with a single tap. The extended settings allow the activation of automatic updates, (interval of between six hours and two weeks), plus the configuration of real-time protection and ESET's Live Grid. The default action to be taken in the event of malware discovery can also be set. There is a choice of "Remove" or "Quarantine".

### Anti-Theft

This has to be activated before it can be used, but ESET provides a very convenient wizard for this purpose. The first step is to create a security password of at least four characters. A password hint can also be added as a reminder; ESET points out that short passwords are less secure. In order to prevent unauthorised deinstallation, ESET prompts the user to make the program a device administrator. After this, the current SIM card is registered as trustworthy. The next step is to enter the phone number of a friend or other trusted person. The text to be displayed

on a locked device can be entered, which we liked. If the software is to be controlled by text message, a password is needed. It is possible to use the existing security password, but ESET recommends creating a different password for this purpose.

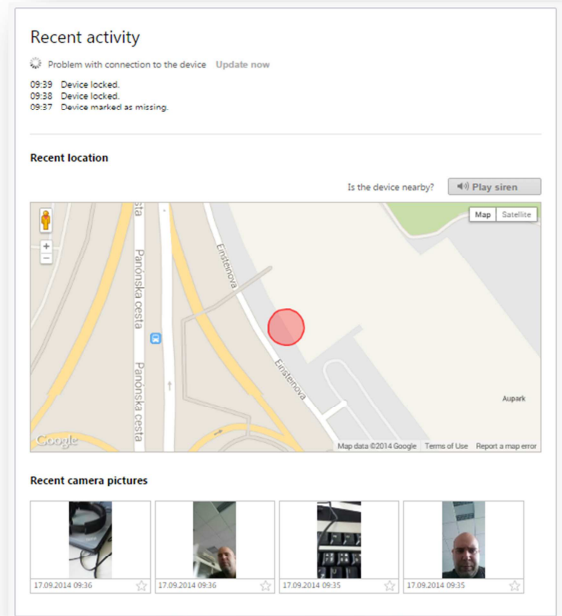


In this year's release, ESET has introduced a web interface for the administration of the product and control of the theft-protection component. A user account for this can be created during the setup process. This concludes the activation of the Anti-Theft component.

The Anti-Theft menu is then displayed on the program's start screen. The "Optimization" entry now stands out, as it has been highlighted in orange, and an exclamation mark indicates that the user's attention is required. If the icon is tapped, ESET informs the user that the lock screen has not been activated. For this reason, the security status is shown as only four out of a possible five stars. Once the lock screen has been set up, the maximum score of five stars is displayed. Other indicators of security are defined by ESET: Location service active, GPS active, screen lock active, mobile data active, Google Play services present.

All the Anti-Theft commands can be given by text message or web interface (<http://my.eset.com>). If the web interface is

used, the device has to be registered as "missing" as a first step before using the theft-protection features. This automatically takes all the important steps required in the event of the device being stolen: the device is locked, its location is registered, and a photo taken, the latter two at regular intervals. We feel this has been very well engineered.



### SIM Guard

This feature is intended to prevent an unauthorised change of the SIM card. If an unregistered SIM is inserted, the smartphone will be locked. This functioned perfectly in our tests. Making an emergency call when the phone was locked would still have been possible, and entering the security password unlocked the phone. A new feature this year is that after five failed password entries, further entries are blocked for a period of time. This is intended to make it more difficult to bypass the lock with brute-force attacks.

### Lock

**Text-message command:** "eset lock <password>"

This command locks the device and thus prevents unauthorised access. If the lock is initiated by text message, the sender will

receive a reply with the IMEI number of the phone and the IMSI number of the SIM card. The lock is robust, we were not able to bypass it. It is possible to make an emergency call, and also to contact the owner.

### Siren

**Text-message command:** "eset siren  
<password>"

This command locks the device and emits a shrill siren at the same time. This may be helpful in simply locating a mislaid phone, e.g. at home, or may encourage a thief to abandon the stolen device.

### Find

**Text-message command:** "eset find  
<password>"

If this command is given by text message, the sender will receive a reply with the coordinates of the phone's location and a link to this on Google maps. If the web interface is used, the device can be continuously tracked. Multiple locations are registered and displayed, making it possible to follow the movement of the phone.

### Wipe

**Text-message command:** "eset wipe  
<password>"

This function is intended to delete all the user's personal data from the mobile phone. The device is not reset to factory defaults, meaning that the theft-protection software remains active after the wipe. In our test, all important data was deleted with the exception of text messages (due to the restrictions of the new OS). On our alternative test device, running Android 4.1.2, the text messages were deleted as expected.

### Other functions

If the device is registered as stolen, ESET's software will automatically take photos with the phone's front camera. These can be viewed in the web interface. This might help identify a thief.

The mobile network to which the device is currently connected is also noted. This helps to identify the phone's location.

Additionally, all this data can be exported and downloaded as a ZIP file. This can be given to the police to aid investigations.







### SMS and Call Filter

This function allows very comprehensive rules to be created for blacklisting and whitelisting calls and text messages. Rules can be created that will block or allow particular communications from particular numbers at particular times. Rules can be created for specific numbers, or for groups such as unknown numbers or hidden numbers.

In our test, ESET displayed a message to say that the blocking of text messages would not work with the operating system on our device. Calls were blocked as expected, however.

### Anti-Phishing

This component protects the user against phishing sites while surfing the Internet. ESET checks the installed browsers for compatibility. According to the manufacturer, the feature works with the most common browsers. In practice, this means that Google Chrome and the Next browser are supported, but others, such as Opera, Firefox, Dolphin and Maxthon are not.

	Chrome Scanned pages: 20	✓
	Next Browser Scanned pages: 0	✓
	Dolphin Browser Not supported	✗
	Firefox Not supported	✗
	Maxthon Browser Not supported	✗
	Opera Not supported	✗

The phishing protection worked perfectly with Google Chrome in our test. If a phishing page



is opened, ESET displays an alert urging the user to leave the site immediately. The Next browser is shown as being compatible, but is not. ESET inform us that they are aware of this and will rectify it as soon as possible.

### Security Audit

The Security Audit feature shows details of system settings and program privileges that could represent a security risk. When we tested this, we were informed that, amongst other things, that the USB Debug Mode and the installation from unknown sources were both activated. The component can also provide alerts regarding unsecured WiFi networks, activated roaming for calls and data traffic, and storage space used.

The Application Audit function assigns apps to one of five groups with regard to possible breaches of privacy. The categories are payment services, location services, obtaining the user's identity, accessing messages and accessing contacts.

### Updates

Updates are carried out automatically. The user can determine the interval. The possible settings are: every six hours, every day, every third day, weekly, fortnightly. Updates can also be run manually.

### Help

For every aspect of the user interface, a comprehensive help service can be opened by tapping the question-mark symbol. This describes the current function in detail.

### Deinstallation

An uninstall wizard is provided, which undertakes all necessary steps to remove the software from the device. The theft-protection password has to be entered first, thus preventing a thief from removing the protection. Thus preventing a thief from removing the protection.

### Licence

There is a free version with reduced functionality; the Premium version costs

€9.99 per year. It includes additional functions such as scheduled scans, phishing protection, automatic malware-definition updates, some theft-protection components (web interface, SIM Guard, Wipe), SMS/Call Filter, and Security Audit.

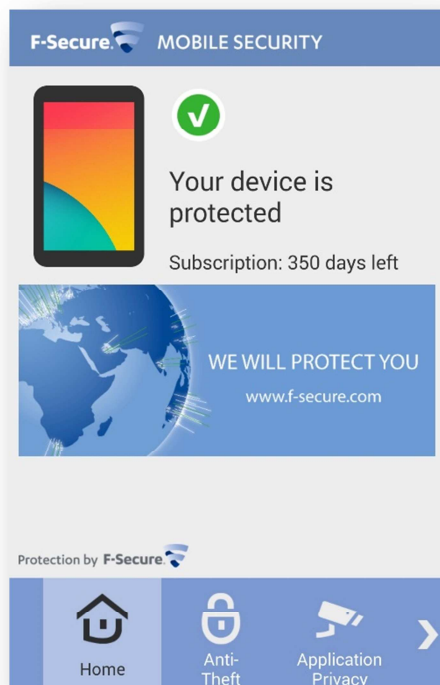
### Summary

ESET Mobile Security stood out in last year's test as a product that combined comprehensive functionality with usability. This year's product is made complete by the addition of the web interface. Our overall impression is of a solid and reliable product.



## F-Secure Mobile Security

F-Secure Mobile Security provides all the important functions of a mobile security product. There are sensible additions in the form of parental control and a web filter.



### Installation

F-Secure Mobile Security was installed from the Google Play Store. The first step of the installation process is to accept the licence agreement. The user can opt out of the default setting to send anonymous usage data to F-Secure.

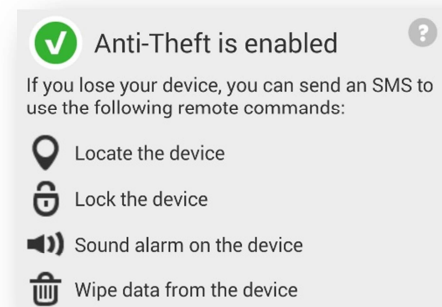
The product has to be activated, whereby a 30-day trial period is possible. The program is made a device administrator in the process of installation. F-Secure recommends running a scan after installation.

### Starting the program

When the program is first started, a message appears, warning that some services have not been activated. This is indicated by the exclamation mark next to the Anti-Theft component.

### Anti-Theft

The theft-protection component is not activated by default. It is controlled exclusively by text message. A web interface is not provided. Before F-Secure's Anti-Theft can be configured, the Android screen lock has to be activated in order to prevent a thief deactivating the protection. A security code has to be entered; this has to have at least 5 characters, and must reach a certain level of complexity. We tried "qqqqq", but this was not accepted. After this, an email address has to be entered for the receipt of instructions, along with a trusted phone number, which will be informed in the event of a SIM-card change. The available text-message commands can be seen in the Help. The password must be entered in order to change settings.



### Lock

#### Text-message command:

**"#lock#<password>"**

This command locks the screen using Android's integrated lock screen. This is very robust and prevents anyone else from accessing the device. When the command has been given, the sender will receive a text message in reply, containing the co-ordinates of the device's current location and a link to this on Google Maps.

### Locate

#### Text-message command:

**"#locate#<password>"**

This function helps the user to find a lost or stolen smartphone.

As with the lock function, the device's co-ordinates and a link to Google Maps will be

sent to the sender's phone by return. The device is also locked. The Locate command is thus de facto identical to the Lock command.

### Alarm

#### Text-message command:

"#alarm#<password>#<count>"

This command works in much the same way as the Lock command, but an alarm is sounded additionally. The *Count* parameter defines how many times the alarm signal should be sounded. Without a number for this parameter, the alarm will sound continuously. It can be switched off by using "0" for the count.

### Wipe

#### Text-message command:

"#wipe#<password>"

The Wipe command deletes all personal data on the smartphone. First, the external SD card is wiped, after this, the device is reset to factory defaults. In our test, all the data was deleted. We were not able to recover data from the external SD card with our normal freeware tool. The whole process was completed in just a few moments.

### SIM Change Lock

This function sends a text message to the registered trusted phone number in the event that the SIM card is exchanged. This could be useful in the event that the SIM card is exchanged by a thief.

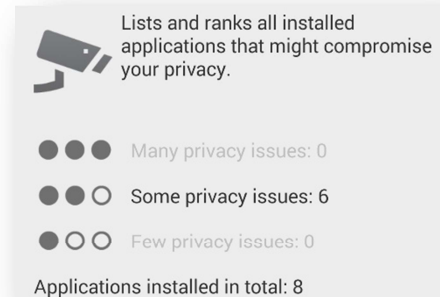
However, in our test this did not work. Despite going through the scenario a number of times, we did not receive a text informing us of the swap. F-Secure inform us that the stolen device's screen will be locked as soon as the phone is restarted after the SIM-card change, preventing access to it. Furthermore, they have reacted quickly and solved the problem in the latest release (9.2.15359).

The function did work properly on our alternative test device with Android 4.1.2.

### Application Privacy

This function scans all installed apps for possible privacy breaches. F-Secure defines

three levels of risk: Many, Some, and Few. Tapping a category in the software displays the apps contained within it. We liked the simplified way that F-Secure uses to display the app privileges. For example, the privilege "ACCESS\_FINE\_LOCATION" is shown in the list as "Knows where you are".



Additionally, a comprehensive description of the privileges is provided. If the user decides that an app is breaching his/her privacy, this can be removed directly from the security software.

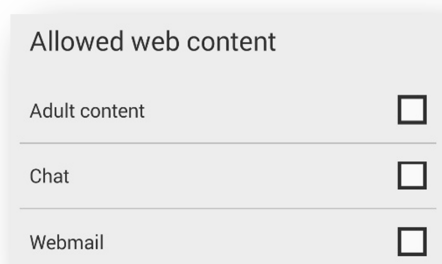
### Anti-Virus

This component protects the system against malware. The data of the last scan and last update are displayed. The device can be scanned manually or automatically on a schedule. The interval for scheduled scans can be set to daily, weekly or monthly. The day of the week and time of day can also be set. Cloud Protection can be deactivated, or set only to run when this would not incur roaming charges. There is also the opportunity to join F-Secure's "Real-Time Protection Network", which is actually activated by default. This analyses files and is intended to protect against the most recent threats. F-Secure state that this involves sending them a file that has been stripped of personal data, in order to continuously improve the service.

### Parental Control

This component serves to keep inappropriate content away from children. Apps unsuitable for children are also blocked. The parent has the choice of three profiles: Child, Teen and

Adult. Each has its own pre-configured filter, and can be individually customised. Categories such as weapons, gambling or illegal downloads can be specified. A password has to be entered to make changes to the parental control configuration, meaning that a child cannot simply deactivate the protection.



The apps that a child can use can also be specified. By default, all installed apps are allowed. Parents can specify individual apps that should be password protected.

### Safe Browsing

F-Secure protects the user against malware and phishing sites while browsing the Internet. To this end, F-Secure's own safe browser is provided. In last year's test, we noted that only the F-Secure browser was protected. F-Secure has improved the product, and now both Google Chrome and Dolphin browsers are also supported. The protection worked well in our test.

### Safe Contacts

This allows calls and texts from specified numbers to be blocked. Numbers to be blocked can be entered manually or imported from the contacts list or call log. This creates a simple blacklist which is used to block the unwanted calls and texts. Outgoing communications to these numbers are also stopped. It is not possible to distinguish between calls and texts for blocking purposes; either both are allowed, or both are blocked. In our test, F-Secure blocked phone calls effectively, but not text messages. However, on our alternative device with an older

version of Android, text messages were also blocked.

### Updates

Updates are carried out automatically. The user can decide whether updates should be downloaded only when the phone is connected via his/her own provider, or also whilst roaming.

### Help

For every function, a help window can be opened by tapping the question-mark symbol. This contains detailed instructions, which should prove entirely adequate.

### Deinstallation

Deinstallation is password-protected. Under the More menu/Uninstall is an uninstall wizard. Once the password has been entered, the program will be removed straight away. To uninstall using the Android App Manager, the suite has to be removed from the list of device administrators; the password has to be entered in this case too.

### Licence

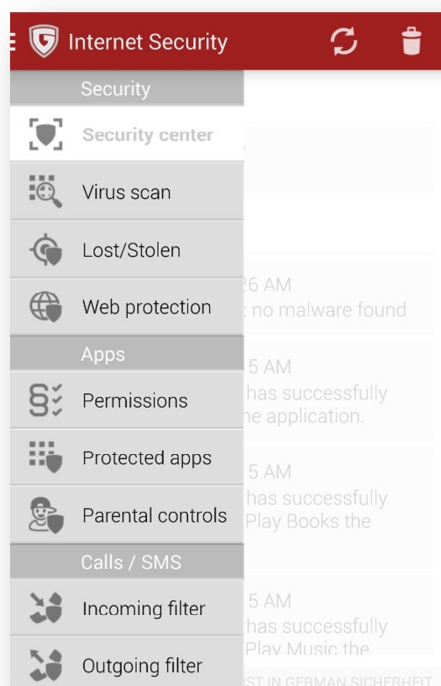
F-Secure allows users to test all the functions of the program free for 30 days. When this time has expired, the user has to purchase a licence to continue using the program. This costs €7.45 for six months.

### Summary

F-Secure gave a good account of itself in our test. We were particularly impressed with the easy navigation and the parental control component. Safe Browsing has been extended to include alternative browsers, which we find very sensible.

## G Data Internet Security

G Data Internet Security provides a malware scanner and theft protection, which is controlled by text message. G Data has also specialised in features for children, such as a special browser for children and a "Children's Corner".



### Installation

We installed G Data's suite from the Google Play Store. The first step is to enter the user's name and email address. An existing licence key can be entered at this stage, or the product can be activated as a 30-day trial version. The user has to accept the licence agreement, and can choose to opt out of allowing personal data to be used for advertising purposes. The theft protection can then be configured. A PIN of at least four characters has to be set. The phone number of a trusted person is requested, which will be used to allow a password reset or receive messages in the event that e.g. the SIM card is changed. G Data Internet Security is then made a device administrator. This completes the setup process.

### Starting the program

When first started, G Data runs an update. The user is notified that an initial scan should be run. There is a choice of scanning just installed apps, or the entire system.

The Security Center, i.e. the program's home screen, then indicates that all is well.

### Virus Scan

The Virus Scan component enables the user to check the smartphone for malicious software. As with the initial scan, there is a choice of scanning just installed apps, or the complete system. The results are shown in the Security Center.

A scheduled scan can be configured in the settings, with a frequency of 1, 3, 7, 14 or 30 days. It can be specified that a scan should only be run if there is sufficient battery life to do so. It is also possible to configure the scan so that it will only run when the device is connected to its charger.

### Lost/Stolen

This feature can help the user in the event that the smartphone is lost or stolen. The functionality is controlled by text messages; a web interface is not included. The user can decide which actions can be started remotely. All are activated by default.

### Locate Telephone

#### **Text-message command: <PIN> locate**

The Locate function establishes the device's position and sends the co-ordinates of this to the sender's phone, along with the MAC address of the router to which the device is connected (where applicable). We feel it would make more sense to provide a direct link to the phone's position on a map service such as Google Maps. We suspect many users will wonder what to do with the co-ordinates, or at least find it inconvenient to have to use them. G Data inform us that they would have to use third-party software to send links to Google Maps (as these are often over the 160 characters available in a single text message), and they prefer not to do this.

As well as the text message, an email is sent to the phone's owner; this does contain a link to Google Maps. The settings contain an option to locate the phone when its battery is low.

### Delete Personal Data

**Text-message command:** <PIN> wipe

This command deletes personal data from the smartphone. The phone is reset to factory settings in the process. When we tested it, the feature worked as intended. However, none of the files on the SD card was deleted.

### Play Ringtone

**Text-message command:** <PIN> ring

This command sounds an alarm on the smartphone. This only stops when the G Data Internet Security app is opened.

### Set phone to mute

**Text-message command:** <PIN> mute

Sending this command results in the phone being set to silent. This worked perfectly in our tests.

### Lock Screen

**Text-message command:** <PIN> lock

This command locks the device using the Android lock screen.

### Set device password

**Text-message command:** <old PIN> set device password: <new PIN>

This command allows the PIN to be changed; the old PIN has to be entered first.

### Remote Password Reset

**Text-message command:** remote password reset: <new PIN>

This allows the password to be reset if it has been forgotten; it will only be accepted from the phone number registered for the trusted person.

### SIM Lock

This component locks the device when the SIM card is changed. The trusted person is

also notified. Optionally, the feature can also be set to locate the phone at the same time.

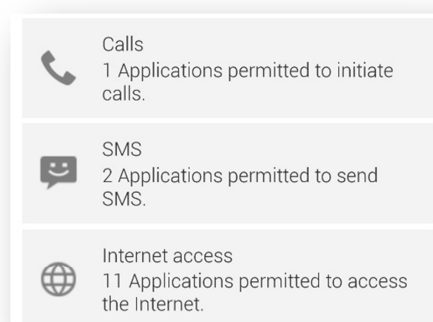
### Web Protection

The Web Protection component protects the user while surfing the web with the standard Android browser or Google Chrome. G Data state that protection is provided against phishing attacks, although this is not possible in the browser's Incognito (private) mode. It can be specified in the settings that Web Protection should only be used when the device is connected to the Internet via WLAN. The component worked well in our quick test.



### Permissions

The Permissions component shows apps with special privileges. Apps are listed according to their permissions, e.g. "Internet Access" or "Location".



Tapping on a category displays all the apps with this permission. Tapping on an app shows its own individual permissions; we did not think this was displayed very clearly. The app can be directly installed from this view, or added to Protected Apps (see below).



### Protected Apps

This prevents unauthorised use of particular apps. An obvious usage case is where parents wish to prevent their children using specific apps which they deem unsuitable. It is thus possible to set a password which has to be entered before a particular app can be used. If the user has forgotten the password, this can be sent by email. It is thus important to protect the email app with a different password, if the email address used for the password reset is one that is synchronised on the device. G Data does not point this out to the user. It is also sensible to password protect the security program itself, in order to prevent it being uninstalled by a thief. G Data does recommend this step, along with password protecting the Android settings and Google Play Store.

### Parental Controls

This enables parents to make the smartphone more child-friendly.



When the component is set up, G Data recommends replacing the standard Android app launcher page with G Data's own app launcher. This covers the Android page, and only shows those apps that the parent has specifically allowed the child to use. The password has to be entered to leave this mode.

This worked fairly well in our test. It was possible to briefly view the list of recently used apps, but not possible to use any of them; it is thus only a cosmetic flaw. The list

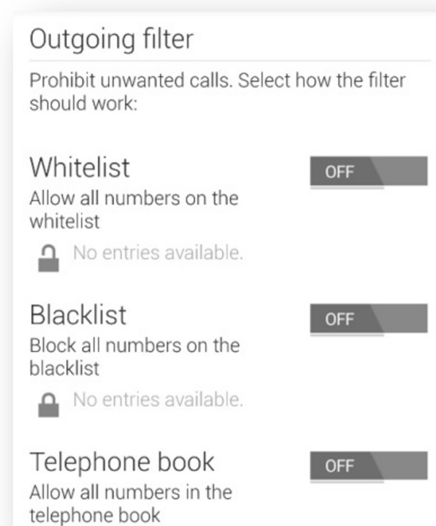
was obscured by the Kid's Corner after a few seconds anyway.

### Kid's browser

The Kid's browser is a separate app, which is intended to provide a safe surfing experience for children. It is only possible to view selected websites (exact list unknown). These are all clearly suitable for children. The browser's home page is <http://fragfinn.de> - this is a search engine that only displays child-friendly results.

### SMS and Call Filter

This element of the application allows unwanted calls and text messages to be blocked. Rules can be created that block incoming calls and texts, and outgoing calls.



Either blacklisting or whitelisting can be used for this purpose. Either blacklisting or whitelisting can be used for this purpose. With blacklisting, the user decides which numbers to block; all others are allowed. It is also possible to allow any and all numbers from the contacts list. A checkbox allows the user to decide whether to accept communications from unknown numbers. In our test, call blocking worked reliably, but it was not possible to block text messages. This is certainly due to the Android version (4.4) on our main test device. On the alternative



phone with Android 4.1.2, the text-message blocking function worked as expected. G Data does not inform the user that the function will not work with the newer Android OS.

Entries for the blacklist and whitelist can be imported from the call log or address book, or entered manually.

### Hide Contacts

The Hide Contacts component of G Data's suite can hide communications from specified contacts, or the contacts themselves. To this end, G Data uses its own messenger program, which takes over the task of sending and receiving text messages.

In our test, this did not work. Both outgoing and incoming messages were shown. Once again, we put this down to incompatibility with the newer Android version. On our alternative device with Android 4.1.2, the function worked perfectly. As with the text blocking feature, G Data does not inform the user of the incompatibility. Hiding the call logs worked perfectly on our main device, however.

### Updates

Updates are carried out automatically. The interval can be set to 1, 3, 7, 14 or 30 days. It is also possible to specify that updates should only be downloaded when the device has a WLAN connection to the Internet.

### Help

Most components provide a short description in the menu, which is usually adequate. We were not able to find a dedicated help function in the form of continuous text or FAQs, however.

### Deinstallation

G Data Internet Security can be uninstalled using the Android App Manager. A password is not required. This could be a problem, as it allows a thief to simply uninstall the theft protection. It is possible to counteract this by proactively configuring the App Protection feature for the Android settings and the security product itself. Whilst G Data

recommends this in the App Protection settings, it is not set up by default.

### Licence

G Data Internet Security is available for €18.99 a year, from the Google Play Store. A "Light" version is available free of charge. This provides protection against dangerous applications, and control of app privileges. It can also be upgraded to the full version.

### Summary

G Data Internet Security's Parental Control feature particularly impressed us, as it appears very well thought-out. A solid theft-protection component is also integrated, although the wipe feature should include the external SD card. The overall impression was sound, however.

## Ikarus mobile.security

mobile.security by Ikarus is a clearly designed security app for Android smartphones. It includes important security features such as a malware scanner, theft protection and URL filter.

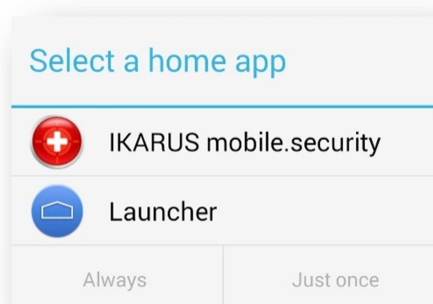


### Installation

We installed Ikarus mobile.security from the Google Play Store. The setup process is relatively long, as it involves setting all the necessary configuration options.

The first step is to accept the licence agreement. Ikarus then runs an update. After this comes licensing. The user has the choice entering an existing key (a QR code can be scanned), making an in-app purchase from the Google Play Store, or activating a 30-day trial version. It is also possible to choose the free version of the product, which has reduced functionality.

The first item to be configured is the theft protection. The user can switch this on or off. If the feature is to be used, mobile.security has to be registered as a device administrator, and also as a "Home App".



It is then necessary to define a password, which has to consist of at least six characters, including at least one letter and at least one number. When this has been done, a brief introduction to the theft protection's text-message commands is displayed. The blacklisting function and URL filter (web protection) are also configured during the installation.

When the setup has been completed, Ikarus recommends running an initial malware scan.

### Starting the program

When the program is first started, its start screen is displayed. At the top of the screen is a status display, which in our case stated "Your system is protected". The dates and times of the last update and scan are shown.

### AntiVirus

Ikarus' antivirus component allows the user to scan all the installed apps, or the entire system. An automatic scan can be scheduled, whereby the possible intervals are twice daily, daily, every second day or every week. Malware detections can be seen in a log.

At the bottom of the screen is a checkbox that allows anonymous malware statistics to be sent to Ikarus; the user can opt out of this.

### Monitoring

This is Ikarus' term for real-time protection, which checks new apps and changes in the file system, and also provides USSD Code protection. Each of the sub-components can be switched on or off independently. By

default, the first two are active, the USSD blocker is not.

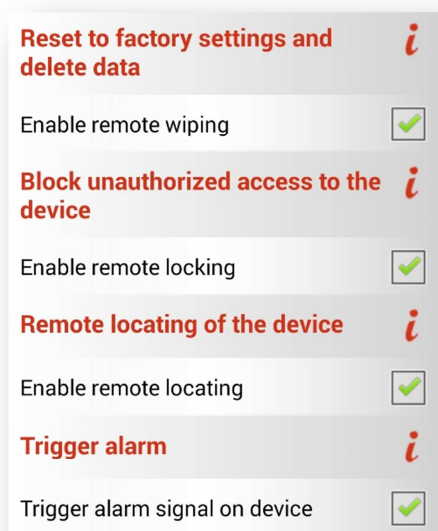
### URL Filter

This protects the user against dangerous websites when surfing the Internet. Ikarus does not state which browsers are supported. It is claimed that phishing pages and sites distributing malware will be blocked.

However, in our functionality test with phishing URLs, no detection was produced.

### Theft Protection

Ikarus lists all the available theft-protection features and allows each component to be activated or deactivated separately. All the theft-protection functions are controlled by text message; a web interface is not provided.



Deactivating each individual component requires the password to be entered. Whilst we welcome this in principle, we feel it would be more practical to demand the password once, to access the entire dialog, rather than having to enter it for each checkbox. This can however be changed in the dialog itself.

### Wipe

**Text-message command: "wipe: <password>" <Password>"**

This command deletes all personal data from the device, meaning that it cannot be accessed by anyone else if the phone is lost

or stolen. This involves resetting the device to factory settings. Ikarus' theft protection deleted the files on an external SD card; however, it was possible to recover them using a popular freeware program.

### Lock

**Text-message command: "lock: <password>" <Password>"**

As soon as this command has been sent, the device is locked using a lock screen. The sender will receive a text message confirming this. The lock screen was very secure, we were unable to bypass it. It was also possible to make an emergency call at all times.

### Locate

**Text-message command: Locate: <password>**

When the phone has been located, the sender receives a reply with the phone's current coordinates and a link to its position on Google Maps.

### Alarm

**Text-message command: "Alarm: <Password>" <Password>"**

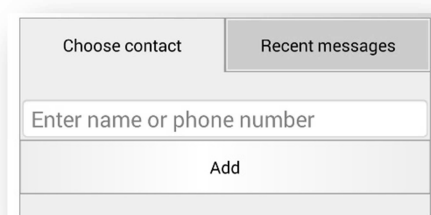
This command is identical to Lock, except that it additionally sounds a loud siren. This works even if the phone is set to vibrate rather than ring.

### SIM Card Protection

If the SIM card is changed, the phone will be locked. It can then only be used if the correct password is entered.

### Message Blacklist

This blocks unwanted text messages by blacklisting senders. The user interface is very simple, and merely allows numbers to be added or removed.



The numbers to block can be entered directly, or imported from the contacts list. It is also possible to add numbers from the text-message log (Recent Messages tab). We liked the fact that a message is automatically sent to the sender when a message is blocked. The text of this can be edited by the user.

In our test, the feature did not work on our primary test device with Android 4.4. We assumed this was due to incompatibility with the newer OS, and this turned out to be true, as the Message Blacklist feature worked perfectly on our alternative device with Android 4.1.2.

### Info

The Info area shows product version information. Contact details for the manufacturer, in the form of email addresses and telephone numbers, can also be found here. It is additionally possible to send the system log to the product support team.

### Restart Setup

This action requires the password to be entered. This resets the configuration of the product and takes the user to the same setup process shown after installation.

### Updates

As with scans, updates can be carried out automatically. The configuration options are also the same. It is also possible to specify that updates should only be carried out when the device is connected via WiFi. It is also possible to run manual updates.

### Help

Ikarus provides the user assistance in the form of concise info boxes. Although there are manuals for other Ikarus products on their website, we could not find one for the mobile suite. There is an FAQ with about 20 questions, although we found these rather superficial.

### Deinstallation

Ikarus mobile.security provides an uninstall wizard to guide the user through uninstalling

the product. The password has to be entered. After this, the user encounters a simple dialog box, and then the product is removed without further ado.

It is possible to uninstall the product using the Android App Manager, in which case the password is not required. Naturally, we regard this as a security problem, as a thief could easily deactivate the theft protection this way.

### Licence

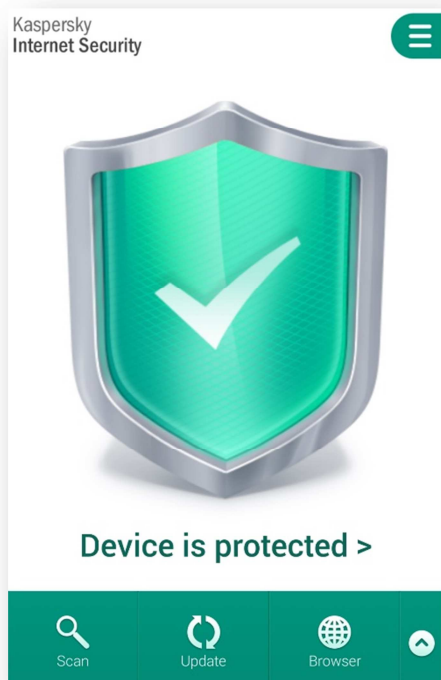
Ikarus allow the user to test mobile.security for 30 days free of charge. When the test period has expired, the user can choose between a lifetime licence from the Google Play Store for €19.95, or a year's licence for €9 from the Ikarus website.

### Summary

Ikarus mobile.security includes all the important security functions. The user interface is very clean and should be easy to use, even for non-experts. The features generally all worked very well.

## Kaspersky Internet Security

This year's version of Kaspersky Internet Security has been given a new look. A wide range of functions is available to the user. As well as a virus scanner, the product includes a text-message and call filter, browser protection, theft protection and more.



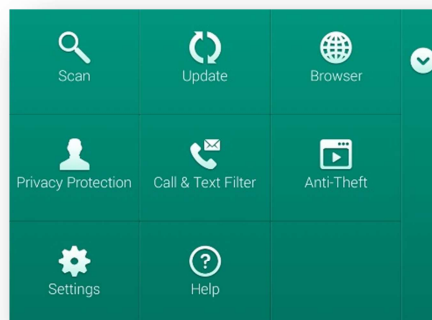
### Installation

Kaspersky Internet Security (KIS) was installed from the Google Play Store. In the first step, the user's country of residence has to be specified. The licence agreement then has to be accepted.

### Starting the program

When installation is complete, the user is taken to the program's home page. There is a very obvious recommendation to carry out a security scan of the device. When this has been done, the home page notes that all is well and the device is protected.

Swiping to the right displays an overview of protection status data, with details of the last scan, update status and licence details. By swiping up from the bottom, the user can display an overview of the available functions:

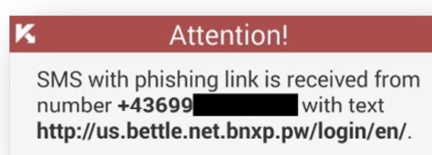


### Scan

This allows the user to scan the device with KIS, to look for malicious software. Three possible variants are offered: Quick Scan searches all installed files, while Full Scan covers the entire device. Folder Scan allows a specific directory to be scanned.

### Browser

Kaspersky provides browser protection to protect the user while surfing the Internet. Kaspersky Lab state that this protects against both phishing and malware. Google Chrome is recommended as the standard browser. We could not find any information regarding any other supported browsers. Another component of the web protection guards against phishing links sent via text message.



This worked well in our test. An alert was shown, stating that access to the phishing page had been blocked.

### Call & Text Filter

When this function is first used, KIS displays an alert stating that due to technical limitations in combination with Android 4.4, there may be problems with sending and receiving text messages. The user has to accept this warning before proceeding.



Due to technical limitations of Android 4.4, the Call & Text Filter functionality of sending and receiving messages may work not as intended.

☐ I agree

A very simple dialog box is then shown. Blacklists and whitelists can be used to specify numbers to be blocked and allowed, respectively.

Kaspersky offers different modes of blocking: *Blocked Contacts* blocks all numbers on the blacklist. *Allowed Contacts* allows texts and calls only from those numbers on the whitelist; all others are rejected. In *Standard Mode*, all numbers on the blacklist are rejected, and all numbers on the whitelist accepted. For numbers that are not on either list, a dialog box is displayed, asking the user how to proceed with the caller.

For the blacklist, the user can specify whether to block only calls, only texts, or both. Numbers can be entered manually, or imported from call/text logs.

In our test, the call-blocking function worked exceptionally well. There were however problems with text messages, as had been warned of. We found that the function worked unpredictably. Behaviour such as this is clearly less desirable than not having a filtering function at all. On our alternative test device with Android 4.1.2, the text-blocking function worked well.

### Privacy Protection

When this function is activated, there is again a warning from Kaspersky Lab that there may be problems sending and receiving messages with the current Android version, 4.4.

The user then has to accept a licence agreement, which principally concerns the use of the user's private data. After this, KIS must be made a device administrator. It announces that it should ideally be the only program with device administrator privileges, and thus suggests removing Google Play Services from the list. This step can be skipped, however. A

Kaspersky Account then has to be registered. This requires an email address and a password with at least 8 characters, including lower-case letters, upper-case letters and numbers. Finally, the user is prompted to define a security code with 4 to 16 characters. Kaspersky Lab recommend writing this down and storing it in a safe place, and also using keys that are at least seven characters long.

When activation is complete, the configuration menu for Privacy Protection is displayed. This module allows specific contacts in the address book, along with texts and call logs, to be hidden. The contacts to be hidden can be defined using a simple menu.

This component worked largely very well in our test. The contacts and call logs were hidden. Text messages could still be seen in the Inbox, however. The names of the senders could not be seen, however, having been hidden in the address book. Deactivating Privacy Protection requires the entry of a PIN. It is possible to configure the program so that contacts are automatically hidden after a certain time.

### Anti-Theft

Kaspersky Lab's theft protection can be controlled using a web interface (<http://anti-theft.kaspersky.com>). Text-message commands are also available, although had considerable difficulty in finding these in our tests.

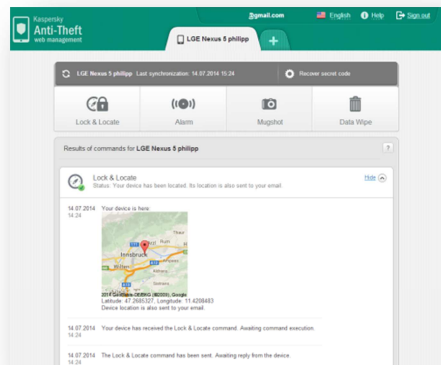
### Lock and Locate

**Text-message command: Find: <PIN>**

This function allows a lost or stolen device to be located and locked. The locate function displays the phone's location on Google Maps. The device is simultaneously locked using Android's own lock screen, which is very secure and cannot be bypassed. A user who has forgotten the PIN can obtain a recovery code via the web interface. This is 16 characters long, and allows the original PIN to be read in plain text. We liked the fact that it is possible to display a personalised message



on the lock screen. It would be possible to display contact information here, for example. If a text-message command is used, the sender will receive a text by return containing the co-ordinates of the device's current location. This is very inconvenient, however. It would make more sense to us if a direct link to a map service were provided.



### Alarm

#### **Text-message command: Alarm <PIN>**

This function locks the device and sounds an alarm. This can be useful when trying to find a mislaid phone. Again, a message can be displayed on the lock screen.

### Mugshot

This function is intended to take photos of the thief using the device's front camera. These are then displayed in the web interface. This helps the owner identify the thief. This command can only be sent via web interface, there is not text-message command.

### Wipe

#### **Text-message command: Wipe: <PIN>**

The Wipe function deletes the owner's personal data from the device. This prevents confidential information falling into the hands of unauthorised persons.

Kaspersky Lab offers two different types of wipe. The first of these deletes just the personal data from the device. This includes contacts, messages, calendar entries, and the Google account. The theft protection remains active in this case. In our test, all the data

except the browser history and bookmarks was deleted.

The second variety of wipe additionally restores the device to factory settings. **Text-message command: fullreset:<PIN>** When we tested this, all the data was deleted, although the theft protection was no longer active (this is inevitable). It was possible to recover the data on the external SD card using a common freeware recovery-program.

### SIM Watch

This component recognises when a new SIM card has been inserted (e.g. by a thief). If this happens, the device is locked. Additionally, text and email messages can be sent to previously specified addresses.

The feature worked well in our test. The device was locked, and notifications were sent to the phone number and email address we had registered.

### Updates

Updates can be run manually by simply tapping the start screen. Automatic updates can be set to run every day or every week, without any additional action being required by the user. The time of day for the update can also be set.

### Help

Kaspersky Lab offer a very extensive help feature. This offers enough assistance to cope with any problems that may arise. In most dialog boxes, there is a VERY small question-mark symbol, which if tapped will take the user to the relevant help page for the feature.

### Deinstallation

To uninstall Kaspersky Internet Security, the user must remove the app from the list of device administrators. A password must be entered to do this. This makes sense, as it prevents a thief from simply uninstalling the theft protection. An even more convenient method of uninstallation is offered by the uninstall wizard, which takes care of deactivating the device administrator privilege.

### Licence

The basic functions of KIS can be used without charge. Extended functionality is provided by the Premium version, which costs €10.95 per year. This includes real-time virus protection, web protection, privacy protection, and protection against text-message phishing.

### Summary

This year, Kaspersky Lab has once again provided a good security product for Android. Sensible features such as text-message phishing protection, privacy protection and theft protection impressed us. We would however strongly recommend that Kaspersky Lab sort out the malfunction of the text-message filter with the current Android version.

## Kingsoft Mobile Security

Kingsoft Mobile Security is a free security product, which has been kept as simple as possible in its design. The main GUI is divided into two pages. On the first page are the “Super Energy Saver” and “App Behavior Manager”. With a swipe to the right, the user can access the main menu. This has a behaviour monitor, a nuisance filter that is supposed to block SPAM texts and unsolicited sales calls, a Payment Guard, and a “safe” QR scanner.

When users in China dial numbers or receive phone calls, the Kingsoft App displays which province, directly governed municipality, region or country incoming calls or dialled numbers belong to.



### Installation

We searched for the Kingsoft app on Baidu and downloaded the version that was marked as “Official Version”. The end user license agreement is already marked as accepted. The app is free of charge.

### Starting the program

When the program is started for the first time, a very simple and clear menu with only two

buttons, i.e. “Super Energy Saver” and “App Behavior Manager”, is shown.

### Complete checkup

After opening the app GUI, the user sees in the center of the window a circular display with the results of a complete checkup. The Kingsoft app checks for system leaks, viruses and Trojans, energy-wasting apps, malicious advertisements and malicious privacy-related behaviour. Problems detected by the app can be repaired with a single tap.

In its final diagnosis of our smartphone, the Kingsoft app reported one OS leak that it recommended we should patch immediately. Rovio’s Amazing Alex was reported because it can obtain the phone number of the device, which according to the in-program description can lead to text-message spam.

In the current version of the app, the AV scan is integrated into the complete checkup.



### Super Energy Saver

This tab displays the estimated battery time left. By adjusting running apps, the user can prolong the time until the device needs to be charged again.



### Main menu

The screenshot below shows the main menu. The first menu item is the access to the app behaviour-log. The log displays app behaviour that can be monitored and behaviour that has already been blocked.



In the software settings, the user can activate/deactivate the monitoring of the following: app installations; energy usage of apps; their “advertisement” behaviour; their privacy-related behaviour; malicious web addresses. Use of the cloud scan function can also be set.

The app can be configured to update only when the device is connected to a WiFi network. Sending feedback to Kingsoft can also be restricted to WiFi only. The heuristic engine is still in beta, and the user is

informed that enabling it can reduce the scan speed. In a final sentence, highly visible in red text, the app tells the user that for normal usage the heuristic engine does not need to be enabled.

We were amazed to see the whitelist for malicious apps, which can be found in the settings tab. It should not be possible to move malicious apps to any whitelist. If this is not its true purpose, the description should be adjusted to make clear what it does do.



### App Behaviour Manager (ABM)



On the “App Behaviour Manager” tab, all installed apps are listed. On sub-tabs, apps are listed that may consume too much energy, have in-app advertisements or require permissions considered to be privacy-relevant (such as accessing the SMS logs or call logs).

### Disturbance blocker

The Kingsoft app can also filter spam texts and nuisance calls. As spam texts and uninvited sales calls are still troubling Chinese mobile phone users, such a feature is highly appreciated. Users are willing to participate by e.g. reporting the numbers used for spam texts and unsolicited sales calls. The app correctly identified various mobile and landline phone numbers currently being used for unsolicited sales calls. However, if a local call is made without dialing the area code, the nuisance blocker does not work, and the call is allowed (even if the same number is blocked when the area code is used).

### Payment Guard

Like many Chinese vendors, Kingsoft has added a "payment guard" feature. This feature is designed to keep safe text messages received during online payment transactions with e.g. confirmation numbers. Such texts can either be stored on the payment guard tab, or immediately deleted after the window displaying the text has been closed by the user.

### Update, Help & Uninstallation

Updates are automatic.

Except for the help with the payment guard, all in-program help is easy to understand. No local help or links to online help could be found. Users can send their feedback directly from the main menu and also suggest new functions.

No password is needed for the uninstallation of the app.

### Licence

Kingsoft is available free of charge.

### Summary

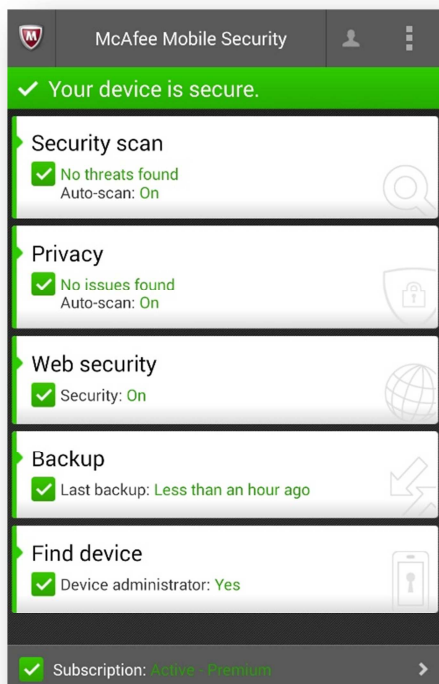
Kingsoft Mobile Security remains an extremely easy-to-use product, but unfortunately still does not have a theft-protection function. We strongly recommend that this function should be added; the danger to a user's privacy in the event of the phone being stolen or lost should not be underestimated.

The integration of the AV scan into the checkup function makes the app easy to use even for absolute beginners.



## McAfee Mobile Security

McAfee Mobile Security provides all the important functions that can be expected of a security product for Android. The free version provides a wide range of features, and a Premium licence is only required for the media upload sub-component of the Backup feature.



### Installation

We installed McAfee Mobile Security from the Google Play Store. The user has to accept the licence agreement; this is the only interaction required of the user.

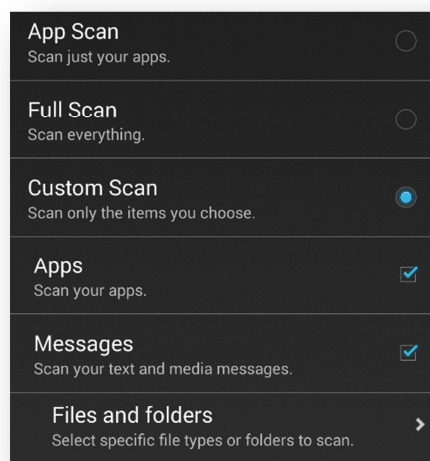
### Starting the program

When the program is first started, both a privacy scan and an initial malware scan are run. After this, the program's start screen is shown. This indicates that the backup function has not been configured. All the other components are shown in green, meaning everything is OK. In our test, an orange "2" character was shown at the top of the screen. Tapping this shows that the two items are (a) activating the lock screen, and (b) installing "McAfee Mobile Innovations". The items are deemed "important". The latter enables the user to test other McAfee apps

that are still at the Beta stage of development. Whilst this may be a nice idea, we feel it should not be described as "important". McAfee inform us that they have taken note of this recommendation.

### Security Scan

This component allows the user to check the smartphone for malicious software. The scan can be set to run automatically. The interval can be set to "daily" or "weekly". The scope of the scan can be set in the options. By default, "Full Scan" is set, but this can be changed to "App Scan" or "Custom Scan".

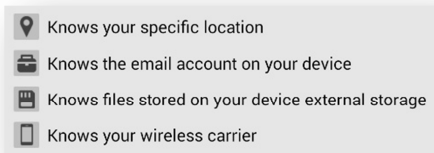


The "App Scan" only checks the installed apps, while the "Custom Scan" provides a choice of apps, messages and individual folders.

### App Privacy

The App Privacy function allows the user to check installed apps for possible privacy violations. All apps are shown in a list, divided into different risk categories. In our test, only apps in the "Medium" and "Low" classes were found. Serious privacy breaches are shown in a separate list, entitled "Notable Apps". Tapping an app in the list displays details of the app and reasons for it being noted as a security risk, e.g. because it can access the device's location data. It is possible to uninstall an app directly from the list.





It is possible to set automatic privacy scans in the settings.

### Privacy Control

This feature protects the user's personal data and repels troublemakers. There are 3 sub-components, listed below.

### Lock Apps

This function enables the user to PIN-protect installed apps. The PIN must be entered to allow access for the use of a protected app. The user can select apps to be locked from a list. In our test, the feature worked as intended; we were not able to use a locked app without entering the PIN.

### Set Profile

McAfee Mobile Security provides four different profiles to choose from: No Limitations, Office, Child, Guest. For each of these profiles, the user can decide which apps will be available for use. In order to block other apps, McAfee has created its own app launcher, which only shows allowed apps. An attempt to go back to the original Android start screen, in order to gain access to all installed apps, requires the PIN to be entered.



This worked well in our test.

### Block Calls

In order to block unwanted calls, McAfee has implemented the Block Calls function. This uses both blacklists and whitelists. In the settings, the user can configure the function with regard to incoming calls, outgoing calls, and roaming. For each of these types, it is possible to specify that all calls be allowed, only whitelisted numbers be allowed, blacklisted calls be blocked, or all numbers be blocked. Additionally, calls from hidden numbers can be blocked if desired.

Blocking text messages is not available for Android 4.4 (KitKat) and higher. However, in our test, we found that when a text message was received from a blacklisted number, a pop-up message appeared, stating that a message from the specified number had been blocked. However, this was not the case, and the manufacturers should deactivate the pop-up to avoid confusion. On our alternative test device with Android 4.1.2, the function was clearly available and worked as expected. It allowed text messages to be blocked using the same filter as for calls, along with text-message filtering using freely defined keywords.

### Web Security

The Web Security function protects the user against malicious websites while surfing the Internet. We ran a quick test of this feature, in which it worked very well.



McAfee also provides a WiFi Security module. This displays a warning in the event that the user connects to an unsecured network.

## Backup

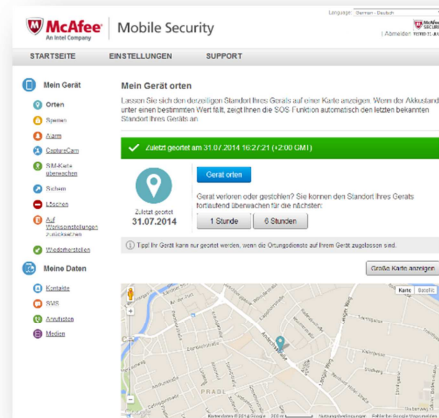
In case the device should be lost or stop working, McAfee has implemented a backup function. This allows text messages, call logs, contacts, and media files such as videos and photos, to be saved to a McAfee server. The backed-up data can be viewed and downloaded via the web interface. Backups can be run manually or automatically. In the latter case, the interval cannot be set, only the option to run backups exclusively over WiFi. A backup of contacts, text messages and call logs can be initiated from the web interface (and also media in the Premium version). This could be useful if the device is lost, as the user can at least back up his or her data.

Contacts and text messages can be restored directly from the phone. When we tested this, we found that we were only able to recover the contacts. We then found a note in the Help, explaining that the data-restore function is not supported with Android 4.4. We re-tested on our alternative device with Android 4.1.2, and the feature worked perfectly.

Another function of the Backup component is the secure deletion of data on the smartphone. Contacts, call logs, photos, videos, and files on the SD card can be deleted. This could be useful e.g. if the user wanted to sell the device.

## Find Device

This menu item takes the user to the theft protection. The function can be controlled via a web interface (<https://www.mcafeemobilesecurity.com>) or by text-message commands.



## Locate

### Text-message command: Secure locate <PIN>

This function locates a lost or stolen device. The phone's position is displayed in Google Maps. If the command is sent by text message, the sender will receive in return a link to a McAfee web page, with an integrated map from Google Maps. We liked the fact that it is possible to track the movement of the device. The device can be located at intervals of one hour or six hours.

## Lock

### Text-message command: Secure lock<PIN>

This command remotely locks the device and prevents unauthorised persons from accessing it. A customised message can be configured in the web interface; this is displayed on the lock screen. This can be useful, as it can provide an honest finder with the owner's contact details, making it possible to return the phone. This can also be changed by text message, using the simple procedure of adding the lock-screen message to the end of the lock command. The Lock function can be combined with the Alarm function, which is explained in the following section.

This function worked extremely well in our test. It was impossible for us to access the Android home screen, notification bar or other view. Additionally, it was always possible to make an emergency call.

## Alarm

### ***Text-message command: Secure alarm<PIN>***

This command sets off a shrill siren, which can be useful if the phone has been mislaid. It can also be used in combination with the Lock function, which may persuade a thief to abandon the phone.

## CaptureCam

### ***Text-message command: Secure alarm<PIN>***

The CaptureCam function uses the device's front camera to take a photo, which is then sent to the user by mail. This allows the him or her to see who is currently using the phone. McAfee have developed a clever method which ensures that the thief's face is photographed, not the inside of a trouser pocket. The basic functionality of this feature is perfectly acceptable, but we wonder why the photos taken with it cannot be seen in the web interface, which shows all other relevant data. We have another, more severe criticism of the feature. In the event that the screen is locked (probably the owner's first action after realising that the device is missing), the clever method of photographing the thief will not work. In this case, the owner is in effect faced with a choice: lock the device OR take a picture of the thief.

## Wipe

### ***Text-message command: Secure wipe<PIN>***

This command deleted the owner's personal data. This does not cause the device to be reset to factory settings, which has the advantage that the theft protection remains installed and active. The owner can choose which data is deleted, for example contacts, text messages, SD card, photos, videos. In our test, all the selected data was deleted, although it was possible to retrieve the data from the external SD card using a popular freeware program.

## Restoring the device to factory settings

### ***Text-message command: Secure reset<PIN>***

This command deletes personal data, as with the Wipe command. Additionally, the device is

restored to factory settings. This means that the theft protection can no longer be used. After carrying out this procedure, we were still able to recover data from the external SD card.

## SIM Guard

This feature locks the device if a different SIM card is inserted. This might happen if a thief inserts his or her own SIM card. When we tested this, the function worked, but we did not receive any notification.

## Updates

Updates can be carried out automatically. This can be configured to run daily or weekly. The user can also run an update manually.

## Help

McAfee provides various Help features. There is an extensive Help page, and every page of the app has an info button; tapping this shows a quick-start guide to the item in question.

## Deinstallation

An uninstaller is provided, which undertakes all necessary steps to remove the product, including removing it from the list of device administrators. A PIN has to be entered, meaning that a thief cannot simply uninstall the theft protection.

## Licence

McAfee Mobile Security is available free of charge from the Google Play Store. A Premium licence is available for €2.49 a month or €29.99 a year; this provides the backup function and telephone support, and removes advertising from the product.

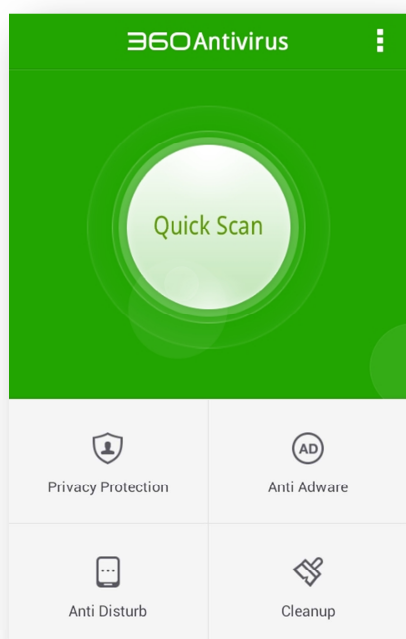
## Summary

McAfee has produced a well-implemented security product for Android, with numerous features. The theft protection is reliable and can be controlled using a web interface. We were happy to see that most of the features were available in the free version.

## Qihoo 360 AntiVirus

Qihoo 360 is a free antivirus product, which includes real-time protection and anti-adware function. However, there is no theft protection. Please note that the Chinese version of the software has a much greater range of functions than the English version reviewed here.

The result reached in this test by Qihoo is not applicable to the English product version available in the Google playstore. Due to the misuse of the award by Qihoo in their related marketing, the award has been withdrawn.



## Installation

We downloaded AntiVirus 360 as an APK file from the manufacturer's website (<http://shouji.360.cn/sd/>) and used this to install the product.



The first step is to accept the licence agreement. Additionally, the user can opt out of the "Experience Improvement Program". The user is then taken to the program's start screen.

## Starting the program

A large button on the program's start screen enables a quick scan to be run. In the upper section of the screen, a message is shown, indicating that "Super Mode" should be activated, in order to enable a number of features.

## Antivirus

The user has the choice of Quick Scan (run from the button on the program's home screen) or Full Scan (run from the context menu). The Quick Scan checks all installed applications for malicious software. The Full Scan additionally checks the memory.

Qihoo's cloud services are used for both scans. This feature is activated by default but can be switched off in the settings. Real-time protection is also provided.

## Super Mode

This mode is required for some functions, such as the Privacy Protector, Ad Blocker, Notification Blocker and Autostart Blocker. However, activating Super Mode does not automatically root the device.

## Tips

Sorry, your phone is not supported yet.

Receive

The attempt to activate Super Mode on our Nexus 5 failed, with a notification that the phone is not currently supported. We were however able to activate the software on our alternative device with an earlier version of

Android. Qihoo inform us that Super Mode will work on a Nexus 5 if the device is rooted.

### Privacy Protection

This component enables particular privileges of installed Android applications to be blocked. In our test, Qihoo announced that it could optimise an app. It noted that a third-party app, File Explorer, needed access to WiFi. The user can decide whether access for this specific app should be allowed or blocked, or whether the user should be asked each time. The program's settings allow a log of past events to be seen.

The feature worked well on our alternative test device with Android 4.1.2, but not on the Nexus 5 with Android 4.4.2.

### Anti Adware

This component removes advertising from apps installed on the device; this is quite different from what we would normally understand by "anti-adware". This too requires the use of Super Mode. Consequently, it was not available on our Nexus 5 test device. However, on the alternative device with Android 4.1.2, the component worked very well. Apps which had previously shown advertising banners became ad-free.

### Anti Disturb

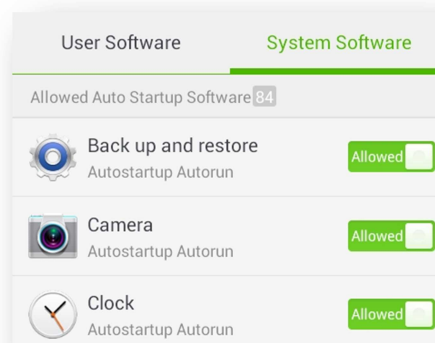
This feature allows alerts in the Notification Bar to be suppressed. It is possible to remove the notification privilege from overly chatty apps. "Leave Me Alone" mode allows only very important notifications to be displayed. It would be nice if this feature could also block alerts at particular times, so that the user would not be disturbed by them e.g. during working hours.

Anti Disturb requires the Super Mode, again meaning that it would not work on our Nexus 5. It worked perfectly on the alternative device with the older Android system, however.

### Block Self-Start Apps

The purpose of this function is to block the automatic execution of apps at system

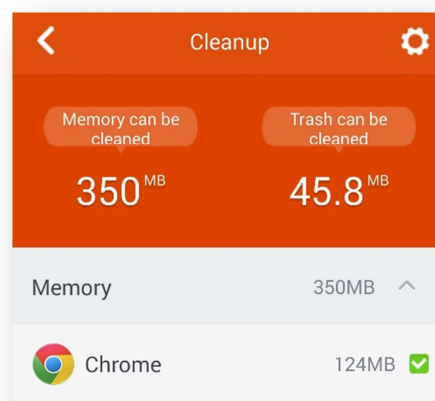
startup. This is intended to prevent slow startup and running of the phone.



The feature's settings display a list of all the apps that start up automatically with the operating system. A simple sliding switch for each app allows the automatic start to be deactivated. This also works for system applications, although Qihoo warns the user to be careful with these.

### Cleanup

The purpose of this feature is to free up RAM and space on the internal storage device. When we tested this, we were able to clean up 350 MB of RAM, along with 4.72 MB of unnecessary cache files and 41.0 MB of superfluous APK files.



### Updates

Updates are carried out automatically. It is also possible to carry out a manual update.

### Help

We were unable to find any form of help for the program.

### Deinstallation

The app can be removed using Android's built-in App Manager. No password is required, but this situation is perfectly acceptable, given that there is no theft-protection feature or similar.

### Licence

Qihoo 360 Antivirus is available free of charge with full functionality.

### Summary

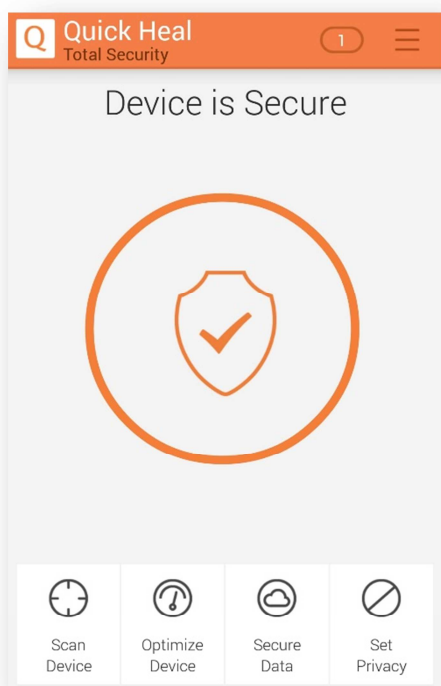
Qihoo provides important functions such as malware protection. Innovative features such as the Anti-Adware component worked extremely well. There is one major problem, however, in that most of the functions require Super Mode. On our Nexus 5 with Android 4.4.2, this mode was not available, meaning that only the malware scanner and clean-up function could be used.

Qihoo has informed us that the latest version of the product now includes theft protection.



## Quick Heal Total Security

Quick Heal offers a comprehensive security product for Android smartphones, which includes all the important functions, such as theft protection, malware protection, and security/privacy advisors. There are also some additional useful features such as Secure Data.



### Installation

The installation file was provided for us by the manufacturer. Once the licence agreement has been accepted, the product has to be activated. If the user already has a licence, he or she can activate the product directly; otherwise, a key has to be obtained.

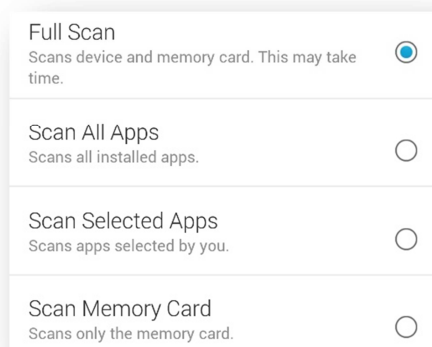
After this, the theft-protection component is configured. A password of between 6 and 20 characters has to be created. The phone number of a trusted person then needs to be entered. This will be used to send notifications in the event that the user forgets the password, or the SIM card is changed by a thief. It is also possible to configure deinstallation protection at this stage. This requires the app to be made a device administrator.

### Starting the program

When setup has been completed, the app's start screen is displayed. Additionally, a system scan is started automatically. The security status is displayed, which in our case was shown as being at 95%. A message states that tapping the display will let the user increase the security level. A menu entitled "Security Measures" informs us that the network monitor, parental controls, automatic backup and "Personal Security" features have not been activated.

### Scan Device

This component allows the device to be scanned for malicious software. The user can choose between a quick scan and a custom scan. The quick scan only checks the installed applications, whereas the custom scan allows the user to select the entire device, only the storage card, only specific apps or only selected folders for scanning.



It is also possible to schedule scans to be run automatically in the future. This feature has been implemented very well. The user can create multiple scan jobs if desired. The time and scope of each scan can be specified, along with the frequency. The options are daily, weekly or monthly. It is also possible to start a scan each time the phone is connected to its charger.

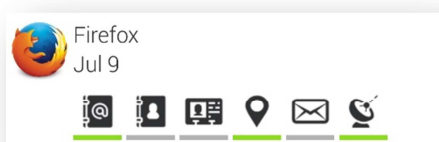
### Security Advisor

The purpose of Security Advisor is to bring to the user's attention any possibly unsafe configurations on the Android smartphone. In our test, the program found fault with 5

settings. It was noted that the device had not been encrypted, and that the screen lock had not been activated. Quick Heal also pointed out that apps could be installed from unknown sources, and that USB debugging had been activated. A simple tap on the cogwheel next to the entry changes the settings to the suggested optimal configuration.

### Privacy Advisor

This component checks installed apps for possible breaches of the user's private sphere. To this end, all installed apps are listed, with icons to indicate which permissions each app has. Tapping an entry displays its details and a short description. A button at the bottom of the screen allows the app to be uninstalled directly.

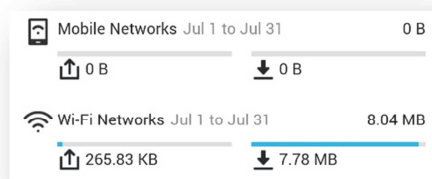


### Optimize Device

This part of the program is devoted to optimising the performance of the device. An overview of the current state of the smartphone is displayed, showing CPU load, battery state and RAM usage.

There is a menu item entitled "Kill Running Apps", which initially just displays a list of currently running applications. These can be sorted by RAM usage or CPU load. Apps can be individually selected using checkboxes, and then closed. There is a whitelist, to which any apps can be added that should be excluded from the "Kill" process.

The feature's Network Summary shows the device's data usage in a graph; this is divided into WiFi and mobile network connections. Additionally, data usage in the last 30 days can be shown for each individual app.



A limit for data usage can be configured. In the event that this is exceeded, Quick Heal can intervene and block the network connection. This can help prevent unnecessary costs, if the user has a limited data volume in his or her mobile phone contract.

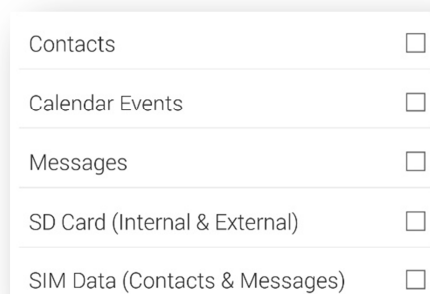
### Secure Data

Secure Data is Quick Heal's cloud backup service. Contacts, calendar entries, messages, photos, music and videos can be backed up. The user is provided with 1024 MB of storage space. There is also a function that will automatically back up the device when it is being charged. The backup cycle can be set to daily, weekly, fortnightly or monthly.

Recovering data is just as simple as backing it up. When restoring text messages, we were shown a notification that Quick Heal had to be registered as the SMS app, in place of Hangouts. When the backup had completed, Hangouts was restored as the default text-message application.

It is possible to delete the backed-up data from Quick Heal's servers.

There is another feature that securely deletes personal data from the phone itself. Contacts, calendar entries, messages, files on internal and external storage, and data on the SIM card are all wiped. This feature may be useful if the user wants to sell the phone.



### Set Privacy

This group includes all the functions that block dangers and spam.

### Call and Message Filter

This component blocks unwanted calls and text messages. As soon as we started the feature, it informed us that text-message blocking is not available with Android 4.4. Numbers to be blocked can be entered manually, or imported from call logs and contacts. It is also possible to block patterns in phone numbers. These can be defined as "Starts with..." or "Ends with...". For each individual entry, the user can block just calls, just texts, or both.

Keywords can be used for text-message filtering. Any text message containing a keyword will be blocked.

Text-message blocking did not work in our test, though this was to be expected, as Quick Heal had warned of it. Rejection of unwanted calls worked as intended, however. On our alternative test device with Android 4.1.2, both call and text blocking worked perfectly.

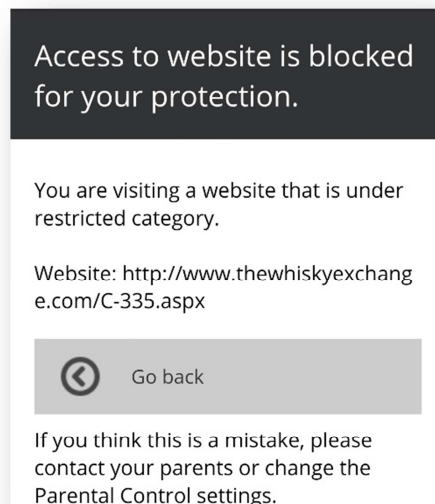
### Privacy Protection

This function makes it possible to hide particular contacts, along with their texts and call-log entries. Again, when starting the function, we were notified that it would not work with text messages under Android 4.4.

Text messages were blocked on our secondary test device with Android 4.1.2, but as announced, not on the newer device with Android 4.4; here, contacts were hidden, and text messages were shown with just the number, not the name. Overall, we would say the function worked well.

### Parental Control

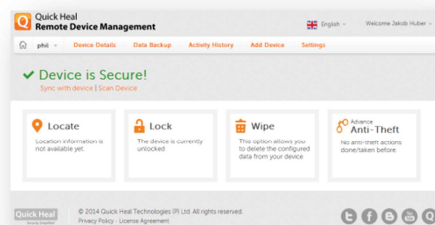
This feature is intended to protect children from harmful content when surfing the Internet. Both blacklists and whitelists are used. For the blacklist, parents can choose from categories such as games, violence or drugs, or enter individual URLs manually. The whitelist defines URLs that should always be allowed.



In our quick test, the feature worked very well.

### Anti-Theft

The theft-protection component can be found in the program's settings. It can be controlled by text-message commands or a web interface (<https://mydevice.quickheal.com>).



The latter is not made obvious by Quick Heal, we had to search for it in order to find it. For the activation of the feature, a "One-time password" (OTP) is sent, which allows the device to be registered.

### Locate

**Text-message command: TRACE <password>**

This function locates the smartphone and shows its position using Google Maps. The device can be continuously located, so that its movements can be tracked.

If the command is sent by text message, the sender will receive a reply with a link to a Quick Heal web page, into which a Google Maps map has been embedded. The co-ordinates are also sent.

## Lock

### **Text-message command: BLOCK <password>**

The Lock function locks the device with a lock screen. This worked very reliably in our test and could not be bypassed. It was also possible to make an emergency call at any time. The trusted contact is also displayed, and can be called directly. The device can be unlocked by entering the password, or by using the web interface.

## Wipe

### **Text-message command: WIPE <password>**

This function deletes personal data from the user's device. On our Nexus 5 (which cannot use an external SD card), all the data was deleted. This did not reset the device to factory settings, with the advantage that the theft-protection software remains active.

On our alternative test device with Android 4.1.2, files on the SD card were also deleted. The program even went to the trouble of overwriting the SD card, meaning that the wipe process took some hours to complete. Unfortunately, this was not successful, as we were able to recover the data using a popular freeware program.

## Dial Call

### **Text-message command: CALL <password>**

This causes the lost or stolen smartphone to call the sender's number.

## Pick Up Call

### **Text-message command: PICKUP <password>**

This command makes the smartphone answer the next call made to it. Unlike the "Dial Call" function, this feature works even if the credit on a pre-paid SIM card is used up.

## Record Audio

### **Text-message command: AUDIO <password>**

When the command has been sent, the device will record sound for one minute. The audio file can then be found in the web interface, in 3gp format.

## Record Video

### **Text-message command: VIDEO <password>**

This records video (using the front camera) and sound for one minute. Again, the result can be found as a 3gp file in the web interface. In our test, it was scarcely possible to recognise anything, as the resolution was very low.

## Ring

### **Text-message command: RING <password>**

This command sounds a siren in the form of a rock song. This could be useful when trying to locate a mislaid mobile phone. The command does not lock the device.

## SIM Change

This function notifies the user by text message when the SIM card is changed. The phone is also locked at the same time.

## Updates

Updates can be run manually, but we were unable to find any more information about automatic updates.

## Personal Security

This feature sends an SOS message to the registered mobile number in an emergency. The user has to press the power button 3 to 5 times to activate the emergency mode. On activation it will send the device location along with an SOS message. The feature will also post a message on social networking sites (Facebook & Twitter).

## Help

Very comprehensive and useful help files are provided. There is also an FAQ page, although this is not very well sorted and so a lot of searching is necessary to find the answer to a particular question.

## Deinstallation

The program can be uninstalled using the Android App Manager. The password has to be entered. This prevents a thief from simply uninstalling the protection. There is also a convenient deinstallation wizard.

### Licence

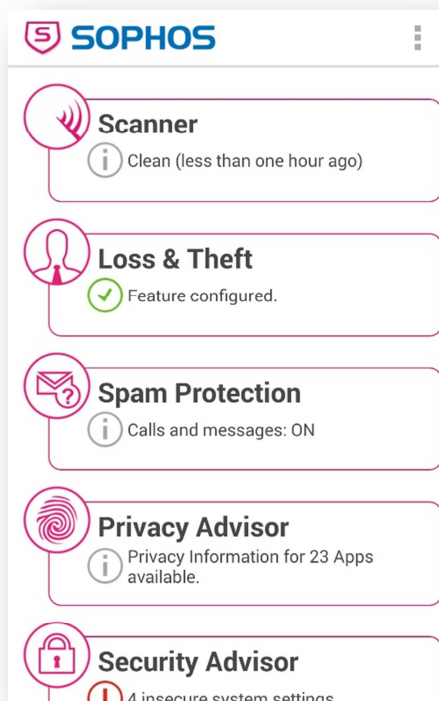
Quick Heal Total Security is available for €5.17 from the Google Play Store.

### Summary

Quick Heal has changed the graphic design of the program considerably from last year's version. The product is one of the most comprehensive in terms of functionality. As well as standard theft-protection features and accompanying web interface, the software offers useful additional features such as backup and parental control.

## Sophos Security and Antivirus

Sophos Security and Antivirus provides all the important components of a modern security product and is available for free.



### Installation

We installed Sophos Security and Antivirus from the Google Play Store. After the installation, the only task is to accept the licence agreement, and then the user is taken to the app's start screen. An initial malware scan is then started.

### Starting the program

The start screen is clearly laid out, making it easy to find one's way around.

### Scan

The scanner searches the phone for malicious software. The user can specify in the settings whether the cloud should be used in scans. There are options to disable cloud support when roaming, or if even if the device is not connected to WiFi. Additionally, it is possible to choose whether scans should check for potentially unwanted applications. Scheduled scans can also be set at intervals ranging from six hours to three days. Sophos also provides

real-time protection, which checks every newly installed app, as well as changes to files.

### Loss & Theft

In the event that the smartphone is lost or stolen, this component can play an alarm, lock the device, locate it, or delete the data on it. Commands are sent by text-message; a web interface is not available. The commands have to be sent from trusted phone numbers, which are defined when the feature is activated. The user also has to create a password to be used when sending the commands. Commands sent from unregistered numbers are ignored, even if the correct password is used.

We liked the clearly designed overview of the theft-protection components, which informs the user which functions are active, and which still need to be configured.

### Lock

**Text-message command: Lock <password>**

This command locks the mobile phone using the Android lock screen. Additionally, an icon with a message about the lock is displayed. The lock screen is very secure and cannot be bypassed. When the device has been successfully locked, the sender will receive a confirmation message in return.

### Alarm

**Text-message command: Alarm <password>**

This command locks the screen, just like the Lock command, but additionally sounds an alarm. This may be very off-putting for a thief.

### Locate

**Text-message command: Locate <password>**

When this command has been sent, the software on the mobile phone will attempt to locate the device, using GPS and WiFi. Once this has been accomplished, the sender's phone will receive a text message with the coordinates and a link to Google Maps. The initial message provides an approximate



position, and is followed some time later with a more exact location.

### Locate at Low Battery

If this function is activated, the location of the device will be reported whenever the battery is low. The position will be reported to the trusted phone number.

### Unlock

**Text-message command: Unlock <password>**

This command defines a new, randomly generated password on the device. The sender will receive a text message containing the new password.

### Wipe

**Text-message command: Wipe <password>**

Sophos has gone to considerable lengths with the Wipe function. The user can define different levels of security for different file types. These dictate whether files should only be deleted (the first 8 KB of each file is overwritten), or completely overwritten with junk files. Unsurprisingly, the latter takes somewhat longer. In our test, this worked as intended. The files on the SD card were deleted and could not be recovered.

### SIM Change

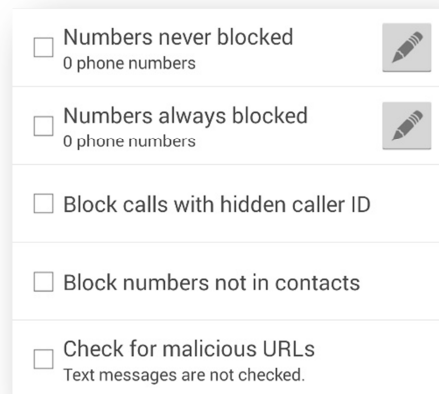
If the device's SIM card is changed, the software will send a message to all registered trusted numbers, containing the IMEI and IMSI of the device. The device will simultaneously be locked using the Android lock screen.

### Spam Protection

This feature protects the user from unwanted calls and text messages. Call blocking and text-message blocking can be activated/deactivated separately from each other. However, the setting then applies globally, i.e. the setting for the blocking function applies to all mails or all texts without exceptions for individual numbers or addresses. An intuitive menu allows the user to create a whitelist, i.e. list of numbers which should never be blocked, and likewise a

blacklist, i.e. list of numbers that should always be blocked. Should the user accidentally enter a number in both lists, the whitelist will take precedence. Users can optionally block calls and texts from hidden numbers, or from all numbers not found in the contacts list.

If the SMS blocker is active, Sophos claims to protect against malicious hyperlinks in text messages.



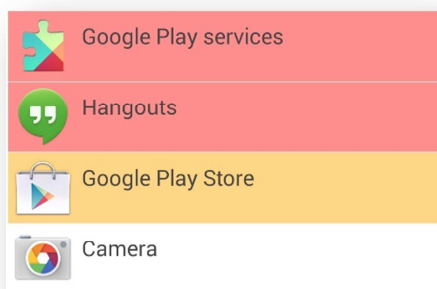
The text-message block function did not work at all on our Nexus 5. However, Sophos informed us about this appropriately. They have also promised to make the software compatible in future releases. On our alternative test device with Android 4.1.2, the function worked exactly as intended.

The call-blocking function worked effectively on both devices, although we noted that the call appears on the screen for a fraction of a second.

The quarantine can be used to view previously blocked calls and texts, and restore or delete them.

### Privacy Advisor

The Privacy Advisor lists installed apps that might represent a threat to the user's privacy. Sophos categorises the apps according to threat level (high, medium, low) and colours the appropriately (red, yellow, white) in the list.



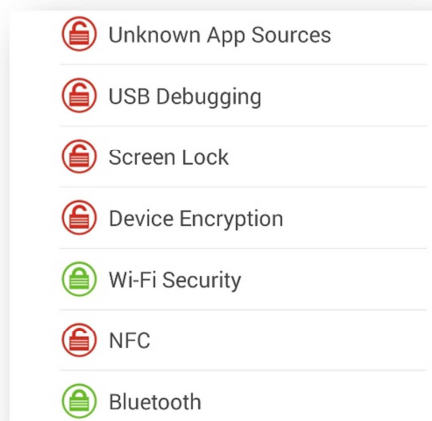
The user can filter the apps according to the following risks: causing costs, accessing personal information, or using the Internet connection. Tapping an application shows very detailed information about it.

### Security Advisor

This points out to the user any settings on the phone that might affect security. Sophos checks seven different settings, including screen lock and device encryption. Tapping one of the entries provides the user with an explanation and a link to the appropriate page in the Android settings.

### App Protection

This component allows installed apps to be password protected using a password of at least four characters. Once this has been set, a warning appears that the App Protection can be bypassed by using the Task Manager. However, Sophos provides help in the form of an additional app, Sophos Security and Antivirus Guard, which ensures that the protection software cannot be stopped. There is a configurable "Grace Period", which defines how long after unlocking the app should be accessible before it is automatically locked again. Sophos has set a default time of five minutes.



As a form of self-protection, Sophos has password protected itself and the Android settings. This cannot be deactivated. From a list of all installed apps, it is possible to choose individual apps to be protected with the same password.

This worked very reliably in our test and could not be bypassed.

### Web Filtering

This component protects the user against malicious websites whilst surfing the Internet. Additionally, undesirable content (e.g. alcohol, drugs, weapons) can be filtered. The component could be used as parental control for a child's smartphone. The configuration page with default settings is shown below:

FILTER MALICIOUS WEBSITES	
Malicious content Containing potential malicious code	Warn
FILTER CATEGORIZED WEBSITES	
Adult Features explicit sexual and pornographic content	Allow
Alcohol & tobacco Promotes alcohol & tobacco products	Allow
Anonymizers Includes sites for anonymous surfing	Allow

Apart from "Malicious content", all other categories have a button marked "Allow". Our initial reaction to this is that the category is currently blocked, and that tapping on it will allow it. In fact, the current status is *allowed*, and tapping the button gives the user the

chance to change the setting to "Warn" or "Block". We find this confusing, and suggest that writing "Allowed" rather than simply "Allow" would be much clearer. We were also confused by the categories "Phishing and Fraud" & "Spyware", as we would expect these to be included in the "Malicious Content" Category. Sophos inform us that these refer to sites that offer advice to criminals on how to create spyware or phishing sites, but are not themselves dangerous to visitors.

Once we had understood how to configure the feature as we wanted, it worked effectively and reliably in our test.

### Updates

We were unable to find any information relating to updates. Sophos merely states that using the cloud scan will always ensure the latest definitions are used.

### Help

Sophos provides the user with a comprehensive help feature for every component, in the form of info boxes. We feel this is adequate.

### Deinstallation

There is currently no uninstall wizard, although Sophos inform us that this is planned for the next version. Security Advisor informs the user that the program must be removed from the list of device administrators before being removed. The app can then be uninstalled using the Android App Manager.

Neither the deactivation of Device Administrator status nor the actual deinstallation itself requires a password to be entered. This would enable a thief to quickly disable the theft-protection software. Activating the integrated App Protection is thus highly recommended, as this does require a password to be entered before the product can be uninstalled. In the current version, there is no explicit mention of this from the manufacturer. However, Sophos is to implement this in the next version.

### Licence

Sophos Security and Antivirus is available free of charge with no restrictions.

### Summary

Sophos made a good impression in our test. The program provides practical features that actively promote security. We particularly liked the Security Advisor, which points out potentially unsafe settings, and the well-designed Spam Protection.

## Tencent Mobile Manager

Tencent Mobile Manager is a free security solution with extensive functionality and numerous optional add-ons. Once again, Tencent has given this tool new features.



### Installing and starting the program

The installation file was downloaded from the official Tencent website.

When the program is first started, the Tencent end-user licence agreement has to be accepted (default setting).

Additionally, the Tencent app encourages the user to configure the Tencent text-message module as the default application for receiving and sending text messages.

After the first start, a "mobile phone health check" is carried out automatically. The resulting health points are displayed in the middle of the "Check-Up & Speed-Up" tab. The user can optimize the device by tapping the circular display. The tuning function ends processes, frees memory and clears out trash files. This brings the health of our device up to 95 points. An additional 5 points are offered for the activation of the payment protection feature.

### Health optimisation tab

On this tab, Tencent offers mobile speed-up, a data traffic manager, and links to download and install an energy manager and a storage space manager.



### Data Volume Manager

Tencent's Traffic Manager displays the daily and monthly data traffic. The monthly data limit according to the user's service contract with the mobile-phone service provider can be entered into the program's settings, so the current data usage can be displayed as a percentage of this. With our Unicom Prepaid card, the check worked as expected.

### Space cleaning

With this feature, Tencent scans the mobile device for WeChat storage, App cache, trash files, OS cache and leftovers of already uninstalled apps. After the standard trash removal, the app tells us to "clean up the WeChat storage manually".



### Energy Manager

“Tencent Battery Manager” is an application that has to be installed separately.

### Storage Manager

The Storage Manager scans for rarely used apps, video files and photos. Photos and video files can be moved to the SD card of the device.

### Security Protection Tab

Under this tab, Tencent lists all available security functions, which are as follows.

#### Nuisance calls and text spam

Tencent has integrated functions to prevent the user being disturbed by nuisance calls and text spam. As well as the usual blacklist and whitelist functions, the software also has a feature that allows the user to report spam messages and nuisance phone numbers to Tencent.

During our test, the feature correctly identified various phone numbers that are currently used for unsolicited phone calls.

#### Payment protection

This feature is designed to provide a safe environment for apps such as Alipay Wallet or WeChat. These apps can be started directly from the payment guard tab. Before the app interface is started, it reports that it is

checking for phishing websites, the QR code and Wifi safety.

### Privacy protection

Tencent Mobile Manager offers a number of privacy protection features, as follows:

#### Privacy Space

A gesture password has to be defined to configure this function. This password is used to hide text messages from specified phone numbers, plus photos, videos and other files. If the user adds e.g. photos to the hidden items, they then appear in their own album within the Privacy Guard tool, but can no longer be seen in the general photo gallery.

#### App permissions

Installed apps are listed according to privacy-related permissions. This function is relevant to finding privacy risks, and apps that may steal personal information.

#### AV Scan

According to the in-program description, the AV-scan function checks for system leaks, malicious apps and payment danger.



In the tab settings, the app can be configured to conduct a “Smart Scan”, “Quick Scan” and “Full Scan”. The user can install an additional Trojan remover tool, which scans the device for specific malware.

#### Anti-Theft

This component is not activated by default. Activation requires the user to configure a password and a trusted mobile phone number,

which will be used to receive an alert in the event that the SIM card has been changed. The theft-protection functions are controlled by text messages. Like many mobile security products, Tencent uses English-language SMS commands.

### Delete

#### **SMS Command: “#QQDeleteALL#password”**

This command deletes personal data from the phone. The phone is not reset to factory settings, with the advantage that the theft-protection software remains active. When we tested it, the delete function removed contacts, text messages and photos from the internal storage.

The Google Account password was not deleted from our test device. As many Chinese users do not use a Google account, this may be seen as a minor risk. On the other hand, Tencent WeChat messages also remained on the device, which was still logged onto our WeChat test account.

### Lock

#### **SMS Command: “#QQLock#password”**

This function locks the mobile phone, to prevent unauthorised access. To unlock the phone, the previously defined password must be entered. In our test, a simple “1” was accepted as security password. Such short passwords provide no protection at all. A text message is sent by Tencent Mobile Manager on successful locking of the phone. After the test, Tencent published a version where the theft-protection can only be used with a QQ account, and using a password is no longer possible.

### Locate

#### **SMS Command: “#QQLocate#password”**

By sending a text message with this command, the user can determine the location of the mobile phone. Whichever phone number sends the lock command will receive in return another text with a written description of the location and a link to the relevant map page of Tencent’s map service.

### Recover password

#### **SMS Command:**

#### **“#QQPin#registered emergency number”**

This function recovers the PIN. It worked fine from the mobile number registered in the theft protection but also from unregistered numbers.

### Program Manager Tab

The Program Manager tab has the features App & Games Download, App Update, Installation Package Management, App Remover and App Permission Manager.



The App & Games Download feature allows the user to browse apps from Tencent’s own App store.

The other features provide update and uninstall management for apps on the device. With the management function for installation packages, the user can reinstall APK files that are still present on the device. Installation files are listed according to the download source, i.e. downloaded from the Tencent download channel or from “Other sources”. The new feature lists apps with permissions such as, among others, sending text messages and obtaining the location of the device.

### Additional tools:

By tapping on the four squares in the upper corner of the GUI, the user can access a variety of other tools such as a mobile-fee scanner. Besides using the tools already installed, the user can download further tools such as a router manager, the Kingsoft battery doctor, and an assistant to move the user’s



files and other private data and to a new smartphone.

There are also security-related features such as an ad detector and a scanner that checks for suspicious text messages relating to payment transactions. The mobile-free scanner reported 10 text messages related to online payments with the taxi app Didi as suspicious. However, texts related to payments with the taxi app Kuaidi were not mentioned. In the update published after the review, this function has been removed.

The WeChat security function probably deserves a more prominent location in the app, as this feature is designed to protect your WeChat account and any messages which are not deleted after a remote data wipe with the #QQEraseAll command of the antitheft protection.

#### **The Tencent rocket**

After installation of the Tencent APP, our test device had a tiny icon at one side of the mobile desktop, obviously intended to display Tencent's measurement of how much memory of the test device was being used. If the user drags this circular display to the bottom of the screen, Tencent closes processes and frees memory.

#### **Deinstallation**

The user is asked for the reason for uninstalling the app, but there is no deinstallation wizard, and no password is required to uninstall the product. This is a problem as regards the anti-theft component, because a thief could simply uninstall the protection.

#### **Licence**

Tencent Mobile Manager is available free.

#### **Help text**

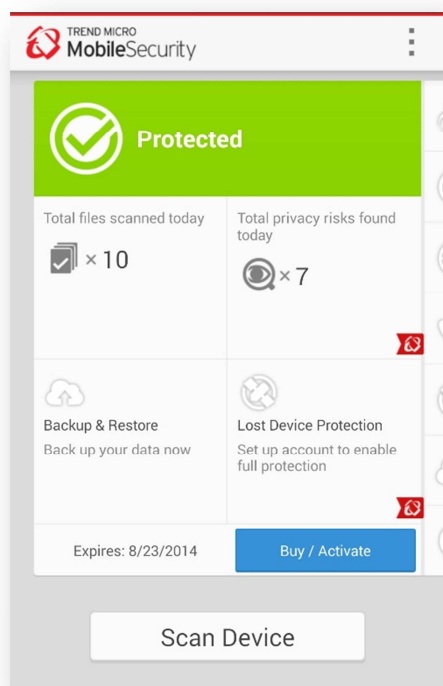
Tencent features are explained within the app with short in-program help texts.

#### **Summary**

Tencent Mobile Manager has a wide range of features, including various anti-theft measures. It was effective at blocking unsolicited phone calls in our test. Suggestions for improvement would be to ensure that the antitheft function really wipes the passwords for Google and WeChat messages along with other data, and to password protect the deinstallation by default.

## Trend Micro Mobile Security

Trend Micro's Mobile Security provides important protection features such as a malware scanner and theft protection, along with useful additions such as safe surfing and parental controls.



### Installation

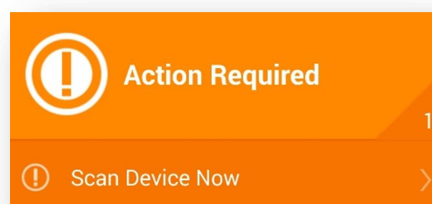
We installed the program from the Google Play Store. Once the licence agreement had been accepted, we were taken to the program's start screen.

### Starting the program

When the program is first started, the user is provided with a brief introduction to the product and its use, which explains e.g. that swiping to the right will bring up advanced functionality. An info box displays a message that the user should log on with their Trend Micro account, or register a new one. A prominent orange box also signals that a malware scan should be carried out.

On Trend Micro's start screen are buttons for accessing results of the malware scanner and data-theft scanner, along with the backup and anti-theft components. In the lower part of

the screen is a prominent "Scan Device" button, which carries out a quick scan.



### Virus Scanner

Tapping the Virus Scan button takes the user to the functionality of this component. There is also a quick-scan button on this screen, along with a multitude of possible settings, such as whether the SD card should be scanned, and if the real-time protection is activated. It is also possible to configure a scan to run each time an update is carried out. The results of updates and scans are listed in a log.

### Privacy Scanner

The Privacy Scanner checks installed apps for risks relating to spying and aggressive advertising. Trend Micro also offers real-time protection for this component, which checks newly installed programs for such threats.

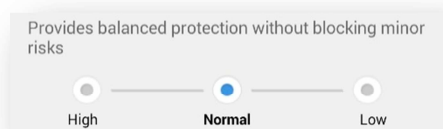


The apps listed below collect your private information or show unusual behavior.

Possible risks are shown in different threat categories. We found the results displayed in our test to be convincing. Questionable apps are thus shown as "Medium Risk", whilst well-known safe apps such as the Opera Browser are deemed "Low Risk". Tapping on an entry in the list displays details of the app's privileges and a brief explanation. Each app can then be uninstalled or added to a list of trusted programs.

### Safe Surfing and Parental Control

This component brings together protection against Internet threats and appropriate web filtering for children.



The Safe Surfing sub-component provides three levels of web protection: High, Medium and Low. The High setting will block sites with the slightest risk, whilst Low is more permissive and ignores minor threats.

Setting up the Parental Control feature requires the Trend Micro account password to be entered. The web-protection for children can then be configured. The user can adjust this for the age of the children concerned. It is also possible to add individual websites to a blacklist or whitelist.



The Uninstall Protection prevents the child/adolescent from removing the program. This feature is useful not only for parental control, but also for theft protection. We would therefore find it more sensible to make it into a global function.

In contrast to last year's version, the Uninstall Protection worked very well in our test. The password was required to uninstall the program, and we were not able to bypass it. There is a log of blocked websites, including both dangerous sites and sites not appropriate for children.

### Call Blocking

Trend Micro enables unwanted calls to be blocked. Either blacklisting or whitelisting can be selected. If whitelisting is used, there is the option to allow calls with hidden numbers.

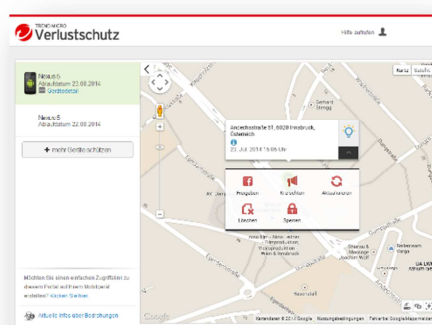
There is also a choice of action to be taken when a call is blocked. "Reject", "Set device to silent", and "Reject and send text-message

reply" are the available options. If the option with text-message reply is selected, there are 3 possible ready-made reply messages, or users can create their own manually.

The text-message blocking feature was not offered on our primary test device, but was shown, and worked properly, on our alternative device with Android 4.1.2. We find this design actually very good, as only those functions that will actually work on a specific device are shown. This is much preferable to displaying a component along with message boxes advising of a malfunction.

### Lost Device Protection

This is Trend Micro's name for theft protection. Standard features such as locate, lock and wipe are provided. The feature is controlled using a web interface; text-message commands are not available.



Changing any of the settings in Lost Device Protection requires the password to be entered, meaning that a thief cannot simply deactivate the service.

### Locate

The Locate function finds the location of a lost or stolen device and displays this on Google Maps. The action is carried out automatically as soon as the user opens the web interface. It is possible to share the position on Facebook.

### SIM Card Lock

This locks the device if the SIM card is removed or replaced.

In our test, it took some time for the SIM lock to take effect. A thief thus has 45 seconds of

unlimited use of the device after it has been restarted.

### Lock

This function locks the device, thus making it inaccessible. It can then only be unlocked with the correct password.

Emergency calls can still be made, and the user can request a new password to be sent by email.

The lock function has been much improved since last year. We were not able to open the notification bar or bypass the lock screen in any way.

### Siren

This command sounds a very loud alarm. The device is not locked, meaning that it is only suitable for locating a mislaid device.

### Wipe

Trend Micro provides two different variants of this function. Partial Remote Wipe deletes personal data from the device, while Full Remote Wipe resets the device to factory settings.

By and large the wipe function worked very well in our test, although we were able to recover a majority of the data from the external SD card using a common freeware program. Trend Micro inform us that a secure wipe would take much longer, and use up more battery power. We would suggest that a quick wipe could be followed by an overwrite process.

### Backup & Restore

This feature is available as a separate app, and allows contacts, calendar entries, call logs, message logs, photos, music and videos to be backed up. Trend Micro provides 50 MB of cloud storage for this purpose.

The backup can be started automatically, with the user able to select the days of the week when it should run. There are options to deactivate the automatic backup when using any mobile data connection (as opposed to WiFi), or when roaming. Restoring backed up data is convenient. The program checks the

data on the server, and suggests which items should be restored.

### Facebook

This function is available as a separate app, and checks the user's Facebook settings for possible privacy risks. This requires the user to enter their Facebook account name and password. All "Privacy Concerns" are then listed. Should the user then wish to make changes to the Facebook settings, these can be entered directly into the Trend Micro program, which will then apply them without any further user action being required.

### Updates

Updates can be run manually or automated. In the case of automatic updates, these can be scheduled to run daily, weekly or monthly. It is also possible to specify that updates should only be run when there is a WiFi connection.

### Help

Trend Micro provides comprehensive help for the program. This is detailed, but presented clearly.

### Deinstallation

The program can be uninstalled using Android's own Application Manager. A password is not needed, unless the user has set up the parental control feature. If this is the case, it is not possible to bypass the password entry. As mentioned above, we feel the password protection should be global, to prevent a thief from simply uninstalling the theft protection.

### Licence

The basic version of Trend Micro Mobile Security is available for free. For the premium functions, namely safe surfing, parental control (including deinstallation protection), location, lock, wipe and SIM lock, a licence is required. This costs €19.95 for a year. The premium functions can be tested free of charge for 30 days.

## Summary

Trend Micro provides the user with sensible protection features for Android smartphones. We particularly liked the parental control feature, which we felt was very well designed. We do however feel that the deinstallation protection should be made a global feature, available even if the parental controls are not set up. Trend Micro inform us that they will attempt to do this in the future. We are pleased to see that the suggestions for improvement we made last year have been implemented in this year's product.

## Webroot SecureAnywhere Mobile Complete

Webroot SecureAnywhere Mobile Complete is a balanced security product, which has a feature-limited free version. For users who require more functionality, a premium version is available.



### Installation

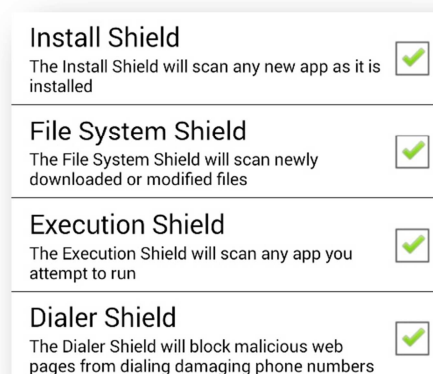
We installed Webroot SecureAnywhere from the Google Play Store. Once the licence agreement has been accepted, the user has to create a Webroot Account or log in with an existing one. The password for the account has to have at least 6 characters. The product is then registered as a device administrator.

### Starting the program

When the program is first started, an alert in yellow points out that the Android lock screen has not been activated, and the installation of apps from unknown sources is allowed. When both of these problems have been fixed, the status display turns green and makes clear that the product is now protected. An automatic malware scan is also carried out.

## Anti-Virus

Webroot's Anti-Virus component is intended to protect the user against malicious software. Various real-time protection features can be activated in the "Shields" settings. These are: real-time protection during installation of apps, file-system guard, app-execution protection, and dialer protection.

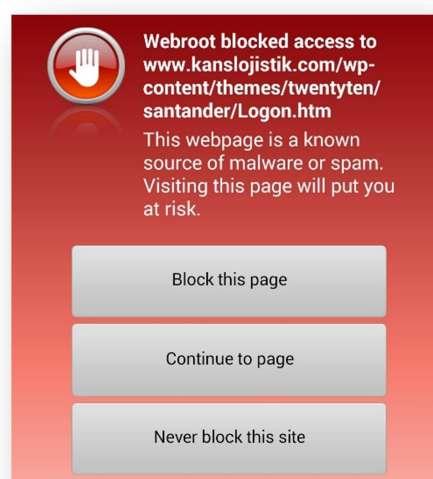


An automatic malware scan is also provided, which can be scheduled to run hourly, daily or weekly. The same applies for updates; these can also be started manually.

## Secure Web Browsing

This feature is intended to protect the user when surfing the Internet. If the user believes that a website has been blocked in error, this can be defined as safe, whereby Webroot will not block it any more.

In our quick test with Google Chrome, this functioned very well.





### Lost Device Protection

The theft protection can be controlled by text messages or a web interface (<https://my.webrootanywhere.com>). The latter is graphically well designed and intuitive to use. It also allows the administration of multiple devices from one account. The web interface displays information on the protection status of each device, along with logs for things such as malware detection.

#### Scream

**Text-message command:** "scream <password>"

This function locks the device, and emits a shrill siren. This can be stopped with a simple tap.

#### Lock

**Text-message command:** "Lock <password>"

This function locks the device in order to prevent unauthorised access. Although the Android lock screen runs in the background and prevents any attempts to bypass it, Webroot's own lock screen is displayed on top of it. This can include a message for an honest finder, which can be edited in the web interface.

#### Wipe

**Text-message command:** "wipe <password>"

When the command has been received, the device is locked, and then personal data is deleted. This resets the device to factory settings. On our alternative test device with Android 4.1.2, files on the external SD card were not deleted.

#### Locate

**Text-message command:** "Locate <password>"

This function serves to find the position of a lost or stolen phone. The device is locked in the process. If the web interface is used to send the command, the device's position will be shown on Google Maps. While the software is in the process of finding the device, no

other commands can be sent. This could create problems if the locating process takes some time.

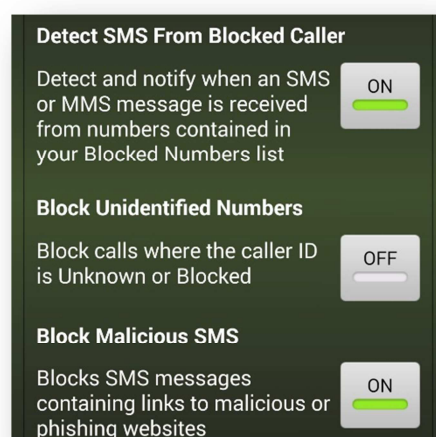
If a text message is used to send the command, the sender will receive a reply with a link to the relevant co-ordinates on Google Maps.

#### SIM Lock

This is only available in the premium version. If the registered SIM card is removed, the device will be locked when it restarts. A thief is thus not able to use the device with their own SIM card.

#### Call & Text Blocking

This component prevents unwanted calls and text messages. The blacklist principle is used. The user can add known troublemakers to a list, which then prevents them making further contact. Numbers can be added manually, or imported from the contacts list, call log or text-message log. It is also possible to block communications from hidden numbers. Webroot also provides protection against text messages with links to dangerous websites. Calls and texts which have been blocked are shown in a clearly laid-out list. The date and content of the messages can be seen, along with the reasons for blocking them.

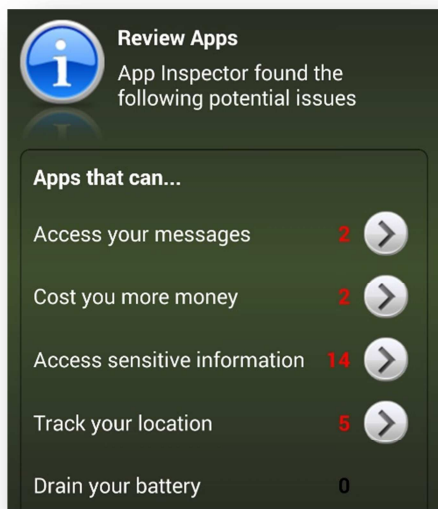


In our test, calls were blocked as intended. Text messages, however, were not. We put this down to incompatibility with Android 4.4; Webroot does not warn the user of this.

Blocking of text messages on our alternative device with Android 4.1.2 worked properly.

### App Inspector

The App Inspector checks installed apps for possible breaches of the user's private sphere. Examples would be apps that have access to text messages, or the phone's location function. Tapping a category of risk shows the relevant applications. No further details of the apps are provided, there is just a link to Android's App Manager.

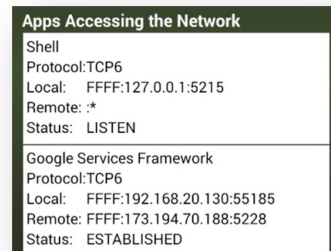


### Battery Monitor

The Battery Monitor provides detailed information about the device's battery, such as charge level, temperature and voltage. The bar graph used in last year's version, showing the battery usage of individual apps, could not be found in the current version.

### Network Monitor

This displays details of apps that use the network. In each case, the name of the protocol, internal and external IP addresses and ports, and the status, are listed. Tapping an entry conducts a "who-is" search of the IP address, and provides details of the Internet service provider, and the approximate position of the device.



### Updates

Updates are carried out automatically. Possible intervals are hourly, daily and weekly. It is also possible to run a manual update.

### Help

Webroot provides a comprehensive help feature for most functions, in the form of a pop-up. An extensive help file is also available.

### Deinstallation

An uninstall wizard is provided to remove the program, which can be done with a single tap. The deinstallation requires the password to be entered, meaning that a thief cannot simply uninstall the theft protection.

### Licence

A reduced-functionality version of Webroot SecureAnywhere Mobile can be used free of charge without time limitation. For users who require more functions, the premium version (which includes uninstall protection, SIM lock, Wipe and various app inspectors) can be purchased. This costs €3.68 for a year.

### Summary

Webroot's Secure Anywhere performed well in our test. Even the free version offers reliable theft protection and various filters which protect the device well. The uninstall protection, SIM lock and various app inspectors make the premium version an attractive proposition. Although some functions, such as the lock, were exemplary, we still feel that some elements of the theft protection should be improved.

## Summary

For some people, smartphones have already replaced the PC. Other users save personal and professional information that could be very interesting for criminals. Phishing is a potential weak point for anyone who uses the Internet, regardless of the type of device used. Credit card details saved in shopping apps or the Google Play Store, as well as the mobile phone contract, can be abused by malware or unauthorised users, resulting in financial losses for the owner.

The potential for attacks is substantial, especially with an open operating system that allows honest developers plenty of scope as regards programming. Unfortunately, creators of malware have exactly the same scope, which they misuse.

Mobile security software protects the users against the majority of these dangers, and has now become indispensable, in our view. Nonetheless, many smartphone users do not protect their devices with such software, and are thus exposed to risks. This is completely unnecessary, especially as a number of products are even available free of charge. Our tests have also largely countered the argument that security products negatively affect the performance or battery life of smartphones.

[illegible]

Feature List Android Mobile Security (as of August 2014)	FREE	COMMERCIAL	FREE	FREE	COMMERCIAL	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	FREE	FREE	COMMERCIAL	FREE	FREE	COMMERCIAL	COMMERCIAL	
Product Name	AhnLab V3 Mobile Plus	avast! Mobile Security	Avira Antivirus Security	Baidu Mobile Security	Bitdefender Mobile Security	CheetahMobile Clean Master	CheetahMobile CM Security	ESET Mobile Security	F-Secure Mobile Security	G Data Internet Security for Android	IKARUS mobile security	Kaspersky Internet Security	Kingsoft Mobile Security	McAfee Mobile Security	Qihoo 360 Mobile Security	Quick Heal Total Security	Sophos Mobile Security	Tencent Mobile Security Manager	Trend Micro Mobile Security	Webroot SecureAnywhere Mobile Complete	
Version Number	2.1	3.0.7751	3.5	5.2.0	2.23.423	5.6.0.1600	1.6.1.1632	3.0	9.2	25.4.0	1.7.21	11.5.4.704	3.3.1.1503	4.2.0.527	2.1.0	2.0.022	3.5.1324	4.8	5.0.0.1247	3.6.0.6610	
Supported Android versions	2.2 and higher	2.2 and higher	2.2 and higher	2.2 and higher	2.3.3 and higher	2.2 and higher	2.2 and higher	2.3 and higher	2.3.3 and higher	2.1 and higher	2.3 and higher	2.3 and higher	2.2 and higher	2.3 and higher	2.2 and higher	2.3 and higher	2.3.3 and higher	2.1 and higher	2.3 and higher	2.2 and higher	
Supported Program languages	English, Korean	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	Chinese	English, Portuguese, French, German, Italian, Polish, Romanian, Spanish, Turkish, Vietnamese	Chinese	English, Russian, Spanish, Italian, Indonesian, Turkish, German, Portuguese, French, Vietnamese, Arabic, Thai, Japanese, Korean, Hungary, Croatian, Greek, Malay, Dutch, Slovak, Bulgarian, Ukrainian, Polish, Serbian, Chinese	English, Russian, Spanish, Italian, Indonesian, Turkish, Swedish, Chinese, Italian, French, Korean, Czech, Hebrew, Slovak, Vietnamese, Arabic, Bulgarian, Thai	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	English, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	German, English, French, Spanish, Portuguese, Italian, Dutch, Polish, Russian, Turkish, Japanese, Chinese	English, German, Italian, French, Spanish, Russian, Chinese, Turkish	English, Russian, German, French, Spanish, Italian, Portuguese	Arabic, Bulgarian, Czech, Danish, German, Greek, English, Spanish, French, Hebrew, Hindi, Croatian, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Dutch, Polish, Portuguese, Romanian, Russian, Slovak, Serbian, Thai, Turkish, Ukrainian, Vietnamese, Chinese	English, Danish, German, Greek, Spanish, Finnish, French, Indonesian, Chinese, Japanese, Korean, Norwegian, Dutch, Portuguese, Russian, Swedish, Turkish, Chinese	English, Chinese	Japanese, Korean, Italian, Spanish, French, German	English, German, French, Italian, Japanese, Chinese	Chinese	English, German, Spanish, French, Italian, Korean, Dutch, Portuguese, Chinese, Turkish, Vietnamese	English, Japanese, Chinese, Dutch, German, French, Italian, Korean, Portuguese, Spanish, Turkish, Russian
Anti-Malware																					
On-Install and On-Demand scan of installed apps	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
On-Demand scan (File system)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
On-Access scan for files	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Scan works offline	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Scan is assisted by cloud	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Automatic (scheduled) Scan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	only on rooted phones	●	●	●	●	●	
Scan installed apps for (possible) privacy violations	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Quarantine	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Recommendations for android settings	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
USSD Blocking	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Anti-Theft																					
Remote Lock & Remote Wipe	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Remote Locate	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Continuous Locate (Track the movement of the phone)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Remote Alarm	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Remote Unlock	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
SMS commands for controlling Anti-Theft features	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Webinterface for controlling Anti-Theft features	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Lock on SIM Change	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Notify on SIM Change (Email / SMS)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Anti-Spam																					
Whitelist / Blacklist SMS	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Whitelist / Blacklist Phonecalls	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Whitelist / Blacklist with wildcards	●	●	●	●	●	●	●	●	●	●	●	●	●	●	only on rooted phones	●	●	●	●	●	
Blocking of SMS containing keywords	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Parental Control																					
Safe WebBrowsing	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
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	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Network monitor	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Local Wipe	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Task killer	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Battery Monitor	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Support																					
Email support	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Online Help	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
FAQ	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
User Forum	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
User Manual	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Phone Support	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Online Chat	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Supported languages of support	English, Korean	English, Czech, French, Spanish, Portuguese, Turkish, Polish, Russian, German, Chinese, Italian	German, English, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malaysian, Korean	Chinese	English, French, Italian, Spanish, Portuguese, Romanian, German, Turkish	Chinese	Chinese	Chinese	All	English, German	German, English, Spanish, Italian, French, Portuguese, Chinese, Japanese	English, German	English, Russian, German, French, Spanish, Italian, Portuguese	Chinese	Spanish, English, Portuguese, Czech, Danish, German, French, Chinese, Italian, Japanese, Dutch, Norwegian, Polish, Russian, Suomi, Swedish, Turkish, Korean	Chinese	Hindi, English, Japanese	English, German, French, Italian, Japanese, Chinese	Chinese	English	All

## Copyright and Disclaimer

This publication is Copyright © 2014 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 2014)