# Mobile Security Review

# Mobile Security Review

Language: English
August 2012
Last revision: 4th September 2012

www.av-comparatives.org

# Contents

## Introduction

Mobile phones are becoming more and more widespread. Smartphones are slowly but surely replacing "just a telephone" devices. In particular, the extensive messaging and Internet functions are becoming ever more popular. This brings some problems, however.

The very features that make smartphones popular also make them interesting for criminals, who attempt to infect them with malware or steal sensitive data. Phishing and similar attacks are particularly threatening.

Using a desktop or laptop PC without security software has become unthinkable. Yet the mobile phone represents a security risk that has been overlooked, despite the fact that it often stores personal data, private photos and sometimes even company data too.

Mobile phones are small but expensive, making them a target for thieves. Security software must make it difficult for thieves to access the data on them, reducing the attractiveness of stealing them. Without protection, criminals have an easy job. After stealing a phone, the thief swaps the SIM card, and the phone is no longer reachable by its owner. Alternatively, they may leave the original SIM card in and make calls at the owner's expense, or use it for further criminal activities. To counteract such scenarios, modern security products for mobile phones are equipped with a range of different features.

### Theft protection

A very useful function is theft protection for mobile phones. In the event that the phone is stolen, the user has the opportunity to locate, lock and wipe the phone. This involves sending a text message to the phone from any other mobile phone, containing the relevant code and a password. In the case of the location function, a text message will be sent back to the sending phone with the GPS co-ordinates of the phone's current location.

This function is very useful, but it should be noted that it is open to being misused to locate the person rather than the phone per se. It is possible to install a security product with a location feature on someone else's phone without their knowledge, or to present someone a phone with location software as a gift.

Some manufacturers allow the theft protection features to be controlled using a web interface, others rely on text messages, and some allow both.

### Malware protection

The malware protection element checks the mobile phone for malicious software, and deletes or quarantines any that it finds. For this function to be effective, malware signatures must be kept up to date. When travelling abroad, users need to take care not to fall into the roaming-costs trap.

Due to the continually growing market share (now 61.0%[1]), we have once again used Google's Android operating system as the test bed for mobile security software this year. The Feature List at the end of the report shows which other platforms are supported by each manufacturer.

In this report you will find details of the products from leading manufacturers who chose to have their programs tested and reviewed by us.

The test was conducted in July and August 2012 under Android 2.3 on a Samsung Galaxy S plus Smartphone.

### Battery usage

Late in the afternoon, a smartphone user might wish they had a portable power station with them. The multiple functions of modern phones mean that even power-saving processors are not able to reduce the battery usage greatly. GPS, email, Internet, and especially the large displays found in most smartphones mean that power usage is high. It can easily happen that heavy use of the

[1] http://www.bgr.com/2012/06/06/smartphone-market-share-2012-ios-windows-phone-idc/

smartphone means that the battery is empty by the afternoon. There are three ways to prevent this. The user can make limited use of the phone, carry a solar-powered battery charger around, or take measures to reduce the power consumption during use as much as possible.

**Display settings:** The display is the greatest user of power in the phone. It makes sense to let the display adjust itself automatically to the ambient light, or to reduce it manually, in order to save power. Some smartphones automatically reduce screen brightness when the battery is low.

**Location:** Switching off GPS saves battery life. Using the function to navigate or localise photos requires the processor to work hard, as the position is constantly being recalculated. We recommend only switching the GPS function on when it's really necessary. The same applies to Wi-Fi and Bluetooth, and indeed any other features of the smartphone; turn it off if you don't need it, and save battery power.

**Multi-tasking:** Under Android, apps may run in the background, in some cases for a long time, without being used at all. Using the Task Manager to close unused apps saves battery life, as they would otherwise be using up power. In Android, the Task Manager can be opened simply pressing and holding the Home button.

### *Exchange, Gmail*

Not only email and contact synchronisation, but also Facebook and other social networks such as LinkedIn update their data from the Internet. Some unknown background services run which can be switched off or changed to a less frequent synchronisation schedule.

Battery life can be extended by a third if email synchronisation is changed from instant to every quarter of an hour. This is also true for status updates from Facebook etc. Every new Facebook update switches the display on and plays an audio notification, both of which use up the battery.

### *Security Software*

Many users are still convinced that security software on an Android smartphone is power-hungry. However, our tests show that this is no longer the case. The effect of security software on battery life can be more or less ignored. Tasks whose power consumption actually is increased by the presence of security software are only rarely used by users who use the phone only for phone calls.

Where the security suite runs backups, e.g. via Wi-Fi, battery usage is extremely high. We were pleased to see that some products in our test only carry out the backup when the smartphone is connected to its charger.

## Summary

The perfect mobile security product does not exist. However, users can find out about the advantages and disadvantages of various products, and make an informed decision on this basis. We recommend installing a free test version and trying this for a few days before deciding whether it is suitable. New versions of security software for Android phones are constantly appearing, with improvements and new features.

We recognise that by participating in our public review, the manufacturers have shown a commitment to providing good mobile phone security for their customers. As this report shows, we found some issues with many of the products, such as bugs or features not working properly. However, the companies concerned are working on rectifying these problems, and indeed some of the issues found have already been fixed. As the core functionality of all of the products was good, and malware detection reached a good standard in all cases, we are happy to approve all of the mobile security suites included in this report.

AV comparatives APPROVED MOBILE PRODUCT SEP 2012

Anyone who wants a free product with many features will find **avast! Mobile Security** to be a very well thought-out security product for their smartphone.

**BitDefender Mobile Security** and **Trend Micro Mobile Security** allow users to simply administer the theft protection of multiple mobile phones from a single web interface.

**ESET Mobile Security** currently contains the most modern security components for smartphones. Additionally, it has obvious appeal for users who use multiple SIM cards in their mobile phones.

Anyone wishing to use parental controls on their own smartphone (or their children's) should take a closer look at **F-Secure Mobile Security**.

**IKARUS mobile.security 2013** and **Sophos Mobile Security** are both simple-to-use security products with the most important basic features.

**Kaspersky Mobile Security** allows the user to protect their privacy by hiding incoming text messages, call history and contacts.

**Lookout Premium** and **McAfee Mobile Security** are amongst the few products to have an integrated backup function, which can be administered from a web interface.

**Qihoo 360 Mobilesafe** is a very comprehensive Chinese product which includes a variety of interesting features, like e.g. optimisation tools, traffic manager and other functions which help users in everyday situations in China.

**TrustGo Antivirus & Mobile Security** is the only product to offer a search for trustworthy apps only. It should be considered by anyone who has security concerns with Google Play.

Anyone who wants to administer their theft protection by text message AND web interface should take a look at **Webroot SecureAnywhere Mobile Security**.

## Tested/Reviewed Products

The following products were reviewed in this report. The manufacturers either provided the most up-to-date version, or confirmed that it was available on Google play at the time when the test/review took place. After the review, the manufacturers had the opportunity to fix any issues/bugs we found, and these improvements are noted in the final report.

- **avast! Mobile Security 1.0**
- **Bitdefender Mobile Security 1.1**
- **ESET Mobile Security 1.1**
- **F-Secure Mobile Security 7.6**
- **IKARUS mobile.security 1.1**
- **Kaspersky Mobile Security 9.4**
- **Lookout Premium 7.14**
- **McAfee Mobile Security 2.1**
- **Qihoo 360 Mobilesafe 3.1**
- **Sophos Mobile Security 1.0**
- **Trend Micro Mobile Security 2.5**
- **TrustGo Antivirus & Mobile Security 1.1**
- **Webroot SecureAnywhere Mobile Security & Antivirus Premier 2.9**

## Battery usage

Measuring the battery usage of a device would at first glance appear to be very easy. When one takes a closer look, however, it becomes apparent that there are difficulties. In particular, the way individual users use their mobile phones can vary greatly. Some make use of the phone's multimedia capabilities; others use the phone to read documents, while some still just use it as a phone. We need to distinguish between power users, who take full advantage of the phone's technical capabilities and functions, and "traditional" users who just use it for phone calls.

In order to find the right balance of telephone usage for this test, we conducted a survey in April 2012. Over a thousand smartphone users from all over the world were asked to respond anonymously to our questions about how they used their phones. It became clear that most users take full advantage of the capabilities of their phones. 95% surf and mail with their phones, over 66% listen to music over the Internet or watch online videos. It is noteworthy that 70% of users never switch their phones off.

Smartphones are becoming more and more important, and very few users leave any function of their phones unused. The smartphone is becoming the omnipresent means of communication, an extension and even replacement of the computer. Telephony is becoming more of a background function, with over 41% of users spending 10 minutes or less actually talking on their phones. 29% of the users spend more than an hour a day on the Internet.

The answers from our mobile security survey (April 2012) were used as the basis for our usage statistics. This data was used to form the typical daily usage patterns for the battery-life test.

### Environmental conditions

To measure the battery usage (battery drain) precisely, we worked with x.test and Agilent to use an ISO-calibrated measuring device for our tests. This high-precision instrument can measure battery drain exactly. An automated standard test run, emulating real users in accordance with the survey data, was carried out multiple times.

### External influences

In order to exclude environmental and technical influences, we took pains to ensure that each device was tested under exactly the same conditions, compatible with influences ECMA-383[2].

The 3G and WiFi connections are susceptible to variations caused by e.g. the weather conditions. In order to minimise/remove such fluctuations, we put a WiFi base station and our own UMTS base station in our testing lab. We could thus determine that the energy required establishing a wireless connection was the same for each product.

Battery usage is naturally dependent on the type of mobile phone. Various factors influence battery drain, an important one being the nature of the display. A larger screen will of course take more battery power than a smaller one. The type of display (LCD, OLED, AMOLED, etc.) is also relevant. Using the same phone for all test candidates allowed us to rule out any such differences influencing our test.

[2] http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-383.pdf

We measured the power consumption while performing the following task based on average usage (according to our mobile phone usage survey) as follows:

- Making **phone calls** (30 minutes a day)
- **Viewing pictures**/photos with the integrated "Gallery" and with "Picasa" (82 minutes a day)
- **Browsing websites** (stored on a local server to avoid the influence of Internet connection speed fluctuations; 45 minutes a day)
- **Watching YouTube** videos online with the integrated YouTube app (17 minutes a day)
- **Watching locally stored videos** on the device (13 minutes a day)
- **Receiving and sending mails** using the integrated Google Mail client (2 minutes a day)
- **Opening documents** stored on the device, like PDFs and Word documents (1 minute a day)
- Standby

The performance test/battery drain analysis showed that mobile security products have only a small impact on the battery, lower than ~2% a day (when doing the above tasks for the time mentioned above). This means that less than 30 minutes a day of battery power are lost. We consider an impact up to a few percent to be an acceptable amount and therefore we are not providing a ranking (which could get misused by marketing departments), especially as the differences are even smaller if a user doesn't carry out any task except phone calls (and standby). We noticed that all products which rely on the cloud to detect Android malware have a higher impact on battery drain (more than security apps which get updates once a day).

| Vendor | Battery Drain | Vendor | Battery Drain |
|---|---|---|---|
| avast! | 🟩 | McAfee | 🟩 |
| Bitdefender | 🟩 | Qihoo 360 | 🟩 |
| ESET | 🟩 | Sophos | 🟩 |
| F-Secure | 🟩 | Trend Micro | 🟩 |
| Ikarus | 🟩 | TrustGo | 🟩 |
| Kaspersky | 🟩 | Webroot | 🟩 |
| Lookout | 🟩 | | |

| | |
|---|---|
| 🟩 | less than 3% |
| 🟩 | 3 to 8% |
| 🟨 | 8 to 15% |
| 🟨 | 15 to 25% |
| 🟥 | more than 25% |

The battery drain/automated mobile-performance testing-suite that we have developed can in future be used for internal "old version to new version" comparatives. This will assist manufacturers who want to further reduce their impact on power consumption, or check if new features have a higher/more negative impact on performance.

## Detection of Android malware

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[3]. 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”. Also, 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.

**Top 30 dangerous permissions most requested by Android malware**

1. INTERNET
2. READ_PHONE_STATE
3. SEND_SMS
4. WRITE_EXTERNAL_STORAGE
5. RECEIVE_SMS
6. READ_SMS
7. ACCESS_COARSE_LOCATION
8. READ_CONTACTS
9. ACCESS_FINE_LOCATION
10. WRITE_SMS
11. CALL_PHONE
12. WAKE_LOCK
13. CHANGE_CONFIGURATION
14. READ_LOGS
15. WRITE_CONTACTS
16. RECEIVE_WAP_PUSH
17. WRITE_APN_SETTINGS
18. SYSTEM_ALERT_WINDOW
19. CAMERA
20. GET_TASKS
21. WRITE_SETTINGS
22. MOUNT_UNMOUNT_FILESYSTEMS
23. RECEIVE_MMS
24. BLUETOOTH
25. MODIFY_AUDIO_SETTINGS
26. CHANGE_WIFI_STATE
27. WRITE_CALENDAR
28. CHANGE_NETWORK_STATE
29. READ_CALENDAR
30. MODIFY_PHONE_STATE

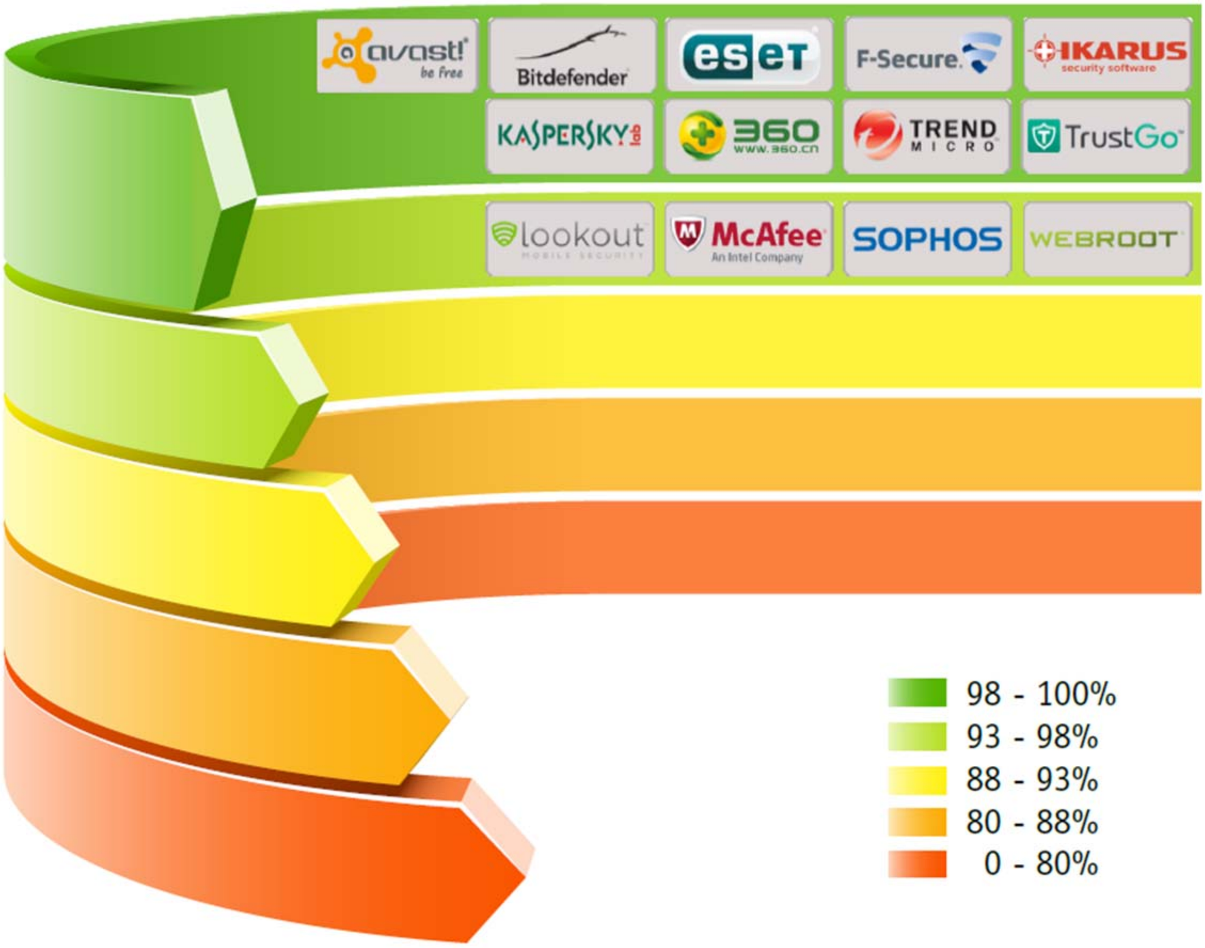
### Test set

In this test, we used only malware and adware appearing or persisting within a limited time frame, in order to represent the current threat state. The Android malware used was collected between March 2012 and the 13th July 2012. This means that the malware test set was limited to 18,021 malicious apps (about 75 main families). The mobile security products were last updated the 14th August 2012.

[3] http://en.wikipedia.org/wiki/Sideloading

The test was carried out on real phones with an active connection to the cloud. The test-set consisted exclusively of APK files. Each single file was first scanned on-demand (where possible); afterwards an attempt was made to install each file manually, one by one. This was done in order to evaluate the products' detection capabilities, as most mobile security products only scan the files during installation. We would like to thank all the students who helped us in carrying out this enormous task. We also performed a false-alarm test based on 200 popular (and not ad-supported) clean applications. None of the products reported any false alarms on those 200 popular apps.

## Test results



## Adware controversy

About half of the apps on Android markets are ad-supported in some way. Some apps containing adware annoy users with messages e.g. on the notification bar, making it difficult for ordinary users to know which app is responsible for showing the ad. There are several dedicated adware detectors on the market; this may be because some mobile security products by well-known vendors do not yet detect adware. For users that want to know which product/vendor detects or warns about adware[4], we tested the security products against a set containing various adware families, to get an idea of which ones report adware and which ones do not. As the inclusion of such a feature is optional (and what constitutes annoying adware is debatable[5]), we do not want to criticise vendors whose mobile security products don't detect adware (although we would prefer the option to detect adware and other potentially unwanted apps to be available to users).

Mobile security products detecting/reporting the most adware families:

- Bitdefender
- ESET
- F-Secure
- Qihoo 360
- Trend Micro
- TrustGo
- Webroot

Vendors with separate adware-detecting apps:

- Lookout (Ad Network Detector - Free)

The following mobile security products currently detect/report only a few adware families:

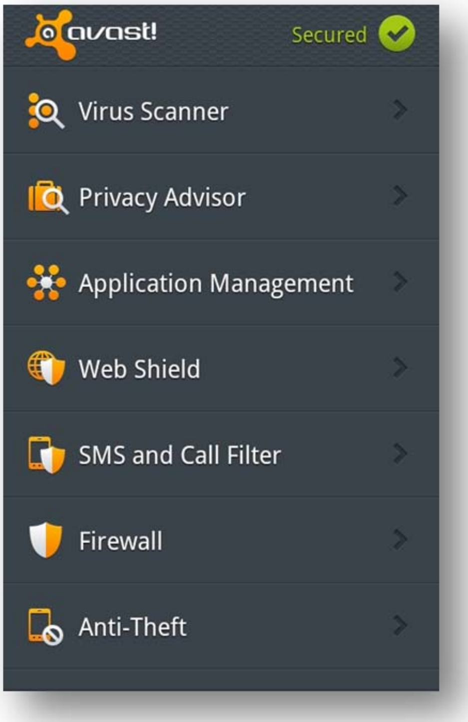
- avast! (adware detection will be included in a future version)
- Ikarus
- Kaspersky
- McAfee
- Sophos

[4] http://dottech.org/android/75309/google-bans-notification-bar-ads-such-as-airpush-from-play-store

[5] http://www.computerworlduk.com/news/security/3333573/lookout-rubbishes-symantec-android-malware-claim

## avast! Mobile Security

With avast! Mobile Security, avast! offers a comprehensive security product for mobile phones, tablets and the like. It is free of charge. Its key features include an antivirus module and browser protection, as well as an anti-theft module.



### Installation

avast! Mobile Security is available free of charge on Google play. After a successful download, we were able to easily install and configure the program using a Setup Wizard. This makes it easy for anyone to perform the installation.

### Starting the Program

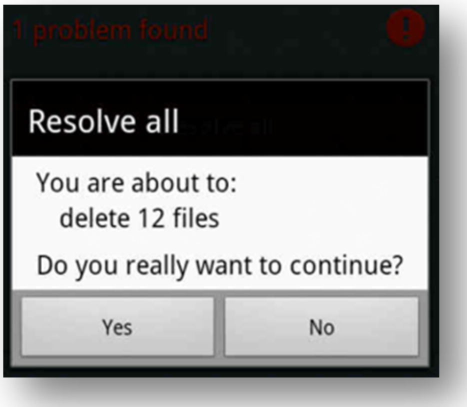
After successfully configuring avast! Mobile Security, the program was started. At first start-up, an initial scan was performed to check installed applications for malware. The update status was only three hours old, so no update was carried out.

Every program start requires entering the password given during installation. Thus, avast! Mobile Security protects itself even before it can be switched off, or the remote control functions can be deactivated by anyone unauthorized.

### Virus Scanner

As with most security products, the user has the opportunity to check their mobile phone for malware. This means apps and the SD card can also be scanned. The option of scanning individual folders is not available. To enable scheduled checks, avast! Mobile Security offers to create a schedule. The user can set the individual days of the week and time of day.

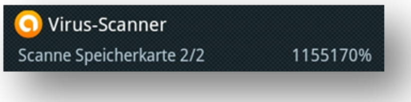
When removing malware, the program in our test crashed several times. Before the crash, the number of found problems with each delete operation was reduced. After avast! Mobile Security was restarted only still outstanding threats were correctly displayed. When the user clicks "Resolve all", a different value is displayed as shown in the screenshot. Also an incorrect value in the progress bar of the virus scanner showed up several times. All those issues have in the meantime been corrected in the new 2.0 version.


1 problem found

Resolve all

You are about to:
delete 12 files

Do you really want to continue?


Virus-Scanner
Scanne Speicherkarte 2/2 1155170%

### Privacy Advisor

The Privacy Advisor categorizes applications which need special permissions such as "give access to messages". As a result, the user receives an overview of possible privacy issues on their mobile device.

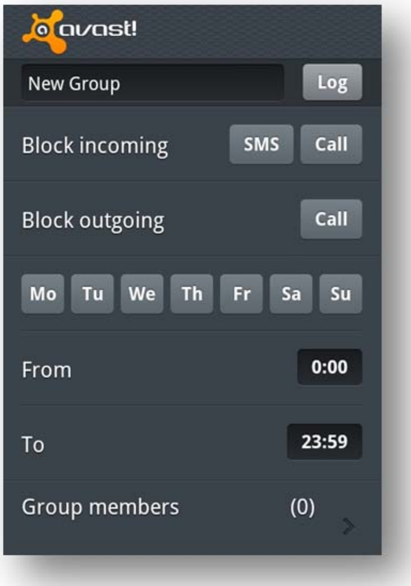
## Application Management

Running applications can be analysed and closed with the help of Application Manager.

## Web Shield

In order to protect the user from attack while surfing on the Internet, avast! Mobile Security is equipped with what it calls Web Shield. This is enabled by default and works exclusively with the Android browser.

## SMS and Call Filters



To avoid disturbance by unwanted calls or text messages, avast! Mobile Security offers the SMS and Call Filter. Here, groups can be created to block calls and text messages at particular times from particular members.

Members in a group can be contacts from the address book, telephone numbers, all anonymous callers and unknown parties.

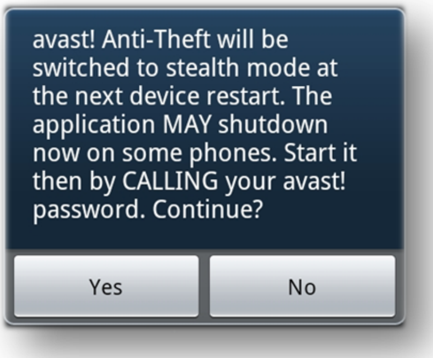
## Firewall

The firewall is switched off with non-rooted phones and cannot be used. This is normal due to restrictions of the operating system with non-rooted devices.

## Anti-Theft

During the installation of avast! Mobile Security, the user can choose between "basic" and "advanced" settings in the configuration of theft protection. Depending on the selection, specific setup options are available to the user.

The "basic" settings must be specified, for example, the name of the mobile device owner, a 4-6 digit password (numbers only) and the Remote Control.


avast! Anti-Theft will be switched to stealth mode at the next device restart. The application MAY shutdown now on some phones. Start it then by CALLING your avast! password. Continue?

avast! Mobile Security creates an additional application logo for the Anti-Theft component with a false name to conceal the theft protection features from a thief. The name can be changed arbitrarily during installation. By default it is avast! Anti-Theft.

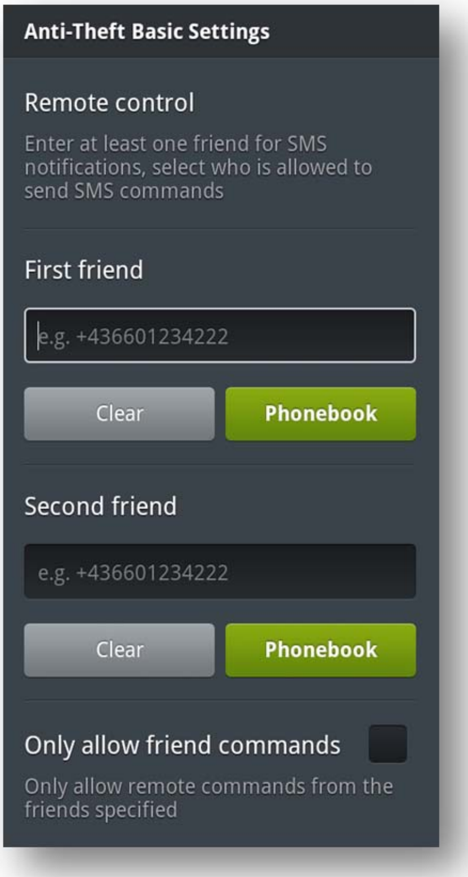
If the user activates Anti-Theft, the application logo is hidden. To make Anti-Theft fully visible again, the user need only call the hidden avast! password on the phone.

Hiding makes sense, for example, if you only uninstall avast! Mobile Security, because the Anti-Theft module will remain and continue to function independently.

Perhaps, it would be a useful enhancement if one could hide the whole suite, so that a thief could not determine whether a security product was installed on the mobile phone or not.

The following configuration guide for the Remote Control caused a little confusion in our team:

"Enter at least one friend for SMS notifications, select who is allowed to send SMS commands"



Anti-Theft Basic Settings

Remote control

Enter at least one friend for SMS notifications, select who is allowed to send SMS commands

First friend

e.g. +436601234222

Second friend

e.g. +436601234222

Only allow friend commands □

Only allow remote commands from the friends specified

According to this instruction, we first thought that only friends' phones can send text commands to the mobile phone. Why are we then offered the checkbox "Only allow friend commands"? After some intensive consideration, we have come to the conclusion that the guide is better understood in two parts. That is why we would split the guide as follows:

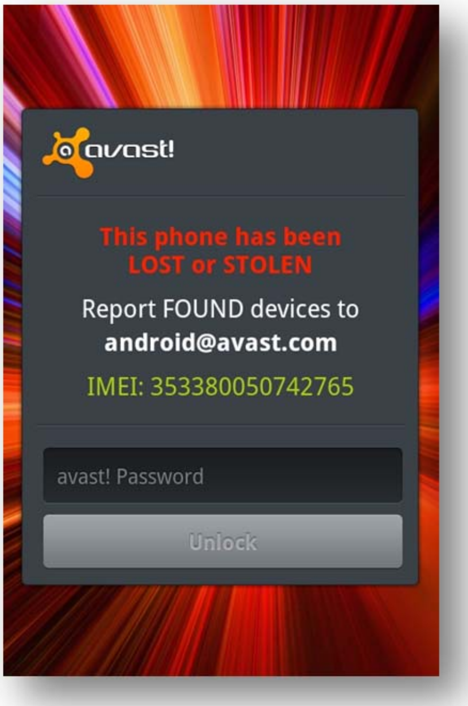
At the top we would only mention "Enter at least one friend for SMS notifications". For the "Only allow friend commands" checkbox we would annotate the second part, "select who is allowed to send SMS commands".

After successful configuration, the user can remotely control their mobile phone with a variety of SMS commands.

We have listed here only the most important commands. A list of all available commands is available at http://www.avast.com/en-us/free-mobile-security#commands.

### Lock Phone

With Anti-Theft activated, the mobile phone can be protected against unauthorized access by sending a text message with the command "password LOCK". Doing so sounds an alarm. Only by entering the correct avast! password can the device be unlocked and the alarm disabled.



This phone has been LOST or STOLEN

Report FOUND devices to android@avast.com

IMEI: 353380050742765

avast! Password

### Location

The current position of the mobile phone can be captured with the command "password LOCATE". The sender receives a text message with a Google Maps link which shows the exact location of the mobile phone. As a bonus, it displays the current cell ID, the country and area code.

### Deletion

avast! Mobile Security differentiates between two types of deletion. In the Anti-Theft settings the user can choose the Normal delete or select Thorough Wipe deletion in the advanced settings.

Both delete modes set our test equipment back to factory settings, which also deleted our personal data.

Thorough Wipe also overwrites the data on the SD card, and data recovery was not possible. In our test, we could determine that exactly 1000 files for every 1MB were created. There was also only 1GB of the memory card overwritten.

#### Google account

Access to a Google account was successfully deleted by restoring the factory settings.

#### Data recovery

After a Normal delete, we could recover most of the data with help of a recovery tool.

With a Thorough Wipe, however, it was not possible to restore any data, except a few thumbnails of our photos.

### *Query*

A very well-thought-out enhancement of theft protection is the possibility of querying contacts, texts, and call and SMS logs. We found this to be particularly striking. This data can be queried by sending a particular command to the lost phone and sent back in SMS form to the sender of the command.

### Conclusion

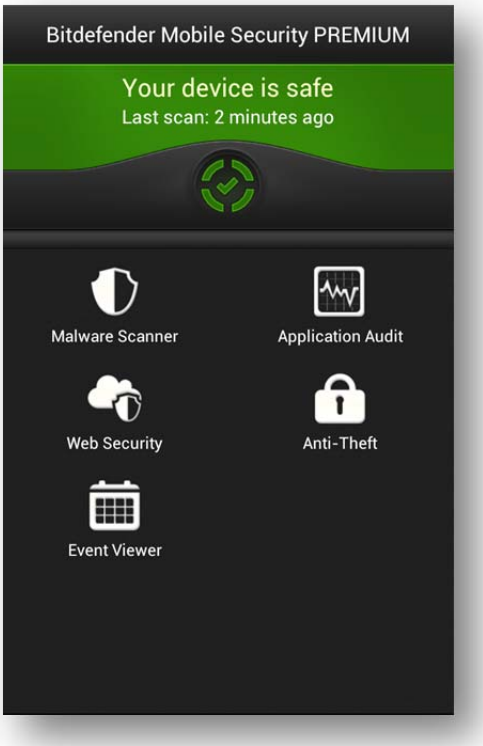
avast! Mobile Security has the most important functionalities available free of charge. What we particularly liked were the number of configuration options and the remote commands, which provide comprehensive remote control for the user.

For users who tend to lose their Smartphones often, avast! Mobile Security is an interesting solution.

The new version 2.0 contains additionally also an Anti-Spam component and can be managed via a webinterface.

## Bitdefender Mobile Security

In its product Bitdefender Mobile Security, Bitdefender brings together a cloud-based malware scanner with anti-theft and web security modules. The anti-theft features can be controlled via a web interface and SMS.


Bitdefender Mobile Security PREMIUM

Your device is safe
Last scan: 2 minutes ago

### Installation

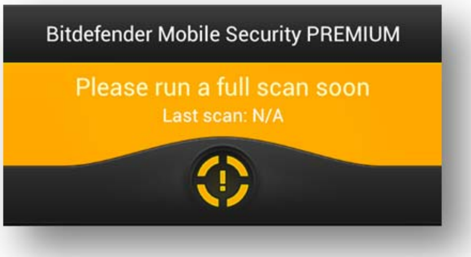
The installation of Bitdefender mobile security was easily managed from Google Play.

Sending anonymous statistics and crash reports is enabled by default when accepting the license agreement.

In the next step the registration via MyBitdefender or a Google account follows. In the future, by using this account, the user can login to the web interface[6] to be able to remotely control the phone.

### Starting the Program

After the successful installation, we could easily launch Bitdefender Mobile Security. The user is immediately urged to perform a virus scan to check the phone for malware. Bitdefender reports nothing on the update status.


Bitdefender Mobile Security PREMIUM

Please run a full scan soon
Last scan: N/A

Only after a successful examination, is the status changed to “Your device is protected”.

No password is necessary to start the application or to change its configuration. This poses a security risk in itself, since then anti-theft can be switched off by anyone. This issue has now been fixed in version 2.0.

### Malware Scanner

Here, the user has the opportunity to check the installed apps and the memory of the mobile phone for malware. There is only one setting possibility offered to the user which starts an automatic scan when you connect the phone to another device.

The malware scanner only works with an operational Internet connection because the cloud is used for the detection.

### Application Audit

The Application Audit module lists all applications that need special privileges, such as access to Internet, private data or commercial services. The applications can be filtered by their associated category to provide an overview.

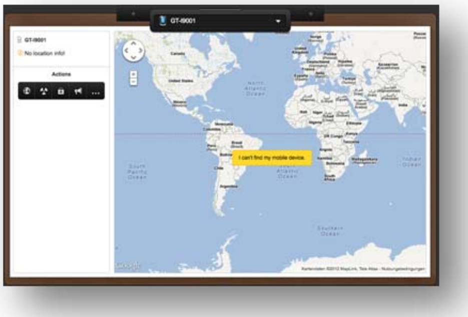
### Web security

The Web Security feature protects the user while browsing with the default Android browser. Bitdefender Mobile Security protects the user from phishing attacks and other malware.

[6] http://my.bitdefender.com

## Web interface

The main anti-theft functions run on the very intuitively designed web interface. It should be noted that multiple mobile devices with the same account can be controlled there. The user has the option of selecting from a list of devices and sending the remote commands to that device.



## Anti-Theft

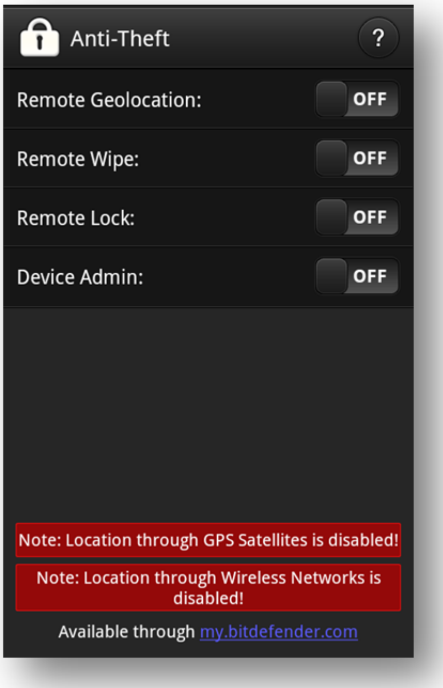
The Anti-Theft initial configuration asks the user to set a PIN number. This PIN will be required for any modification in the Anti-Theft settings as well as for remotely controlling the device through SMS. Features such as remote device detection, remote wipe, remote lock, screan, answer, and call me can be used via the web interface and SMS.

The remote device detection is enabled by default on the mobile-phone-enabled GPS or location through the wireless network. Out-of-the-box, however, the remote wipe, revocation, and the device administrator are disabled.

### *Remote device detection*

The position of the mobile device was displayed correctly on the map in the web interface.

One thing we noticed is that when the GPS or the location over the wireless network was turned off, a conspicuous message appeared, even when the remote device detection was disabled. In our opinion, the message should only appear when the remote device detection is activated.


Anti-Theft ?

Remote Geolocation: OFF

Remote Wipe: OFF

Remote Lock: OFF

Device Admin: OFF

Note: Location through GPS Satellites is disabled!

Note: Location through Wireless Networks is disabled!

Available through my.bitdefender.com

### *Remote wipe*

For remote wipe, Bitdefender Mobile Security differentiates between two scenarios, which are not described in the help function or dialog box.

Only by carrying out frequent remote wipes could we understand these two scenarios.

**Scenario 1:** When Remote Wipe was enabled and Device Administrator was disabled, only the private data of the user on the phone was deleted.

The SMS and call logs, as well as the Favorites in the browser were not deleted.

**Scenario 2:** With Remote Wipe enabled and Device Administrator enabled as well, the phone was reset to factory settings, clearing all data.

We believe both approaches are useful. It should be described in precise detail what data in which configuration will be deleted.

### Google account

Access to the Google account was successfully deleted in both scenarios. This made access by an unauthorized person to the private data and Google Play impossible.

### Data recovery

In both cases, we were able to restore most of the files by using a recovery tool.

### *Remote lock*

With the help of the web interface, the mobile phone can be easily locked. To do this, the user must define a PIN code which will be necessary later to unlock the device.

### *Sending notifications through web interface*

Through the web interface, the user has the option of sending notifications which are then displayed on the screen of the mobile device. Optionally, an alarm can be sounded in addition.

If the phone has not previously been locked, the alarm can be easily silenced. If the phone has been locked, the alarm will sound and cannot be turned off, however the notification text is no longer visible. This could make it more difficult for an honest person who finds the mobile device to return it.

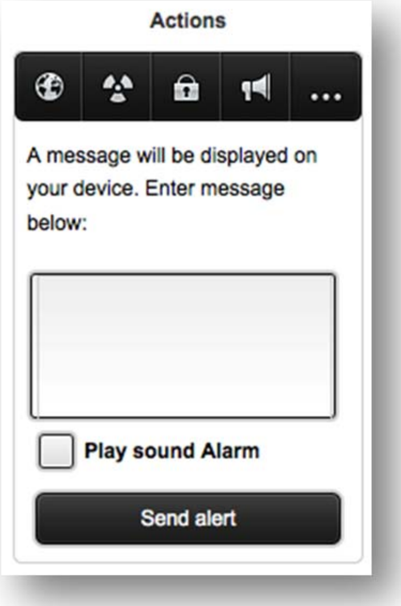
A combination of alarm and lock notification appears to us to be the most sensible.

### *SMS commands*

The available commands are HELP, LOCATE, LOCK, SCREAM, ANSWER and CALLME.

An optional step in the initial configuration for Anti-Theft allows the user to define a "Trusted Number". The trusted number will receive notifications if the SIM card in the phone is changed and is the only number that can send the WIPE command through SMS. All commands worked and the app responded timely to them.

It's also possible to command the device to answer the next call. Once accepted, the device turned on the speaker and turned the screen off. The "answer" command sent returned confirmation from device. Calling the device now automatically picked up the call passing the ambient sounds through. This feature may be helpful to communicate unconditionally with a perpetrator.



Actions

A message will be displayed on your device. Enter message below:

□ Play sound Alarm

Send alert

### Conclusion

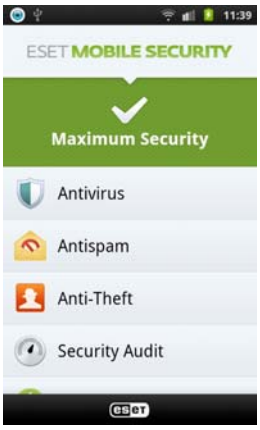
With Bitdefender Mobile Security, the user has a clearly designed security product on his smartphone. This has the major anti-theft features.

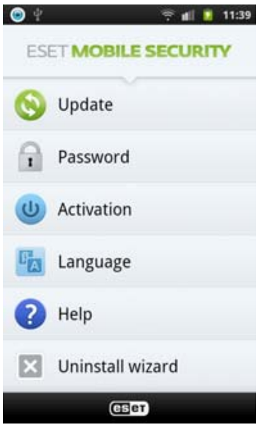
A plus is the intuitively designed web interface which allows a user to connect multiple smartphones with one account.

In terms of the malware scanner, Bitdefender should not rely only on the cloud because with a disabled Internet connection no malware detection is possible.

## ESET Mobile Security

ESET Mobile Security offers a comprehensive security product for mobile phones. The software can be tested for 30 days by anyone without restrictions. Anti-theft, anti-virus and spam protection are among the most important components.





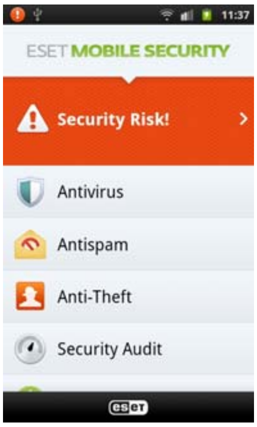
### Installation

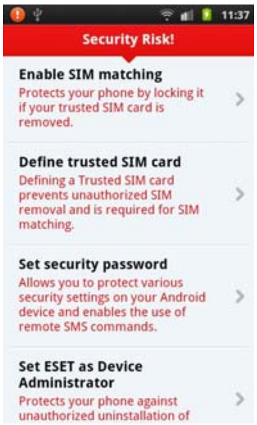
The installation of ESET Mobile Security was performed from Google Play without problems.

### Launching the Program

After accepting the licence agreements, the program was successfully launched. To use all the features, the product must first be enabled. To this end, the user can choose from the options of using a trial licence, licence renewal, entering an existing licence, and licence purchase. After successfully activating it, we were immediately made aware of existing security concerns, such as enabling SIM matching, defining trusted SIMs, setting a security password, etc., it and offered suggestions for solutions.

A single character password could be used to set the security password. ESET is encouraged to prompt the user that short passwords are insecure.





**Enable SIM matching**
Protects your phone by locking it if your trusted SIM card is removed.

**Define trusted SIM card**
Defining a Trusted SIM card prevents unauthorized SIM removal and is required for SIM matching.

**Set security password**
Allows you to protect various security settings on your Android device and enables the use of remote SMS commands.

**Set ESET as Device Administrator**
Protects your phone against unauthorized uninstallation of

When all security vulnerabilities were eliminated, “Maximum Security” was then displayed.

After the initial launch of the program, the virus definition was neither updated, nor was an initial scan carried out. Additionally, the user was not informed about this lack.

### Anti-Virus

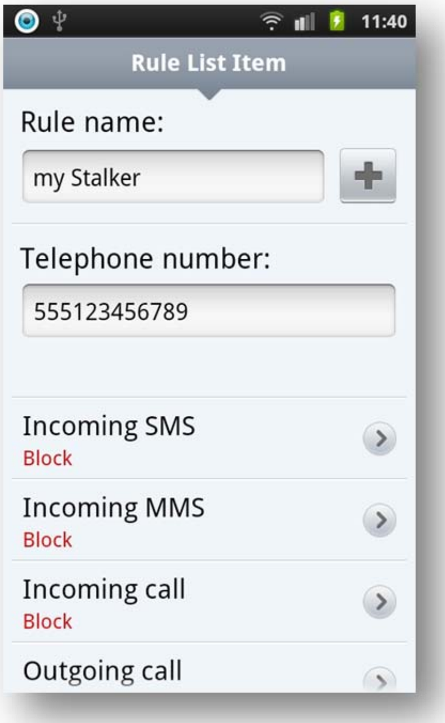
This component allows the user to check the device or freely selectable folders for malware.

In our test, the scans were carried out very quickly, and afterwards displayed a comprehensible overview. The log information can also be called up later under the menu item “Scan Logs”.

Compared to other products, ESET Mobile Security offers a variety of setting options for antivirus protection, and also distinguishes between on-demand and real-time protection.

### Anti-spam

In terms of spam protection ESET Mobile Security used the concept of blacklists and whitelists. Here, the user has the possibility of creating rules with special permissions and adding contacts or phone numbers. The selectable permissions include blocking or allowing incoming text messages, MMS messages, calls, and blocking or allowing outbound calls.



Rule name:

my Stalker

Telephone number:

555123456789

Incoming SMS
Block

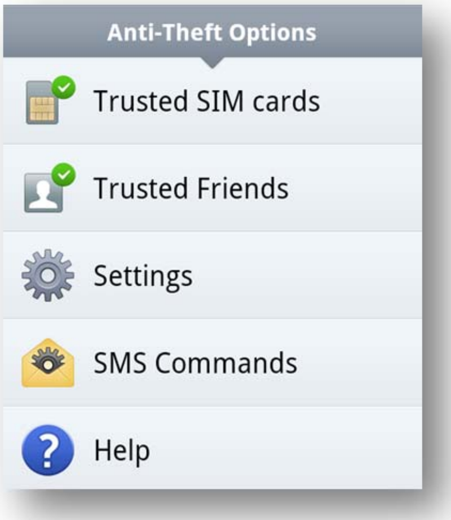
Incoming MMS
Block

Incoming call
Block

Outgoing call

This component appears to us to be very intuitive and easy to use. Contacts from the contact list can be loaded, and the selected rules should apply for their phone numbers.

### Anti-Theft



With the help of Anti-Theft, the user has the ability to remotely control his mobile phone to delete, block and to locate it. To do this, messages with special commands can be sent to the phone.

#### *Trusted SIM*

Here, the user has the ability to define trusted SIM cards, so that exchanging a given SIM does not lock the phone.

#### *Remote Wipe*

All data stored on the mobile phone can be deleted using the command "ESET wipe password". First, the personal information is deleted and the SD card overwritten (not only formatted). Although this operation takes slightly longer, the data are securely deleted. Then, it resets the phone to the factory default settings.

#### Google account

The reset to factory settings makes access to the Google account impossible by any unauthorized person.

#### Data recovery

Because ESET Mobile Security overwrites the entire memory, we were unable to restore any files.

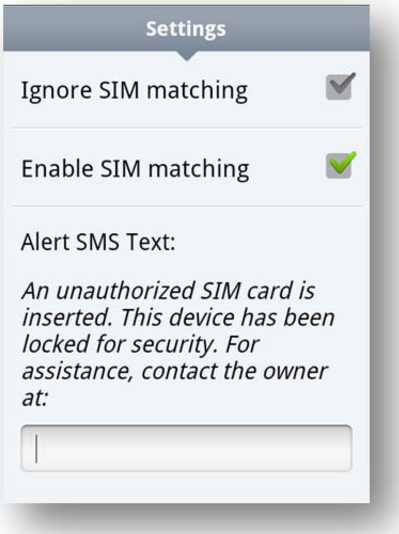
#### *Remote Lock*

The SMS command "ESET lock password" locks the phone. The security password must be entered again to unlock the phone.

The trusted SIM proved to be a very useful setting. Here, the user has the option of registering SIM cards which doesn't trigger a phone lock when a SIM card is swapped. If ESET Mobile Security notices a change to an unregistered SIM card, the phone is immediately locked and an Alert SMS text sent to all trusted friends.

Receiving calls and placing emergency calls was possible without any problems.

### *Settings*



Settings

Ignore SIM matching ☑

Enable SIM matching ☑

Alert SMS Text:

*An unauthorized SIM card is inserted. This device has been locked for security. For assistance, contact the owner at:*

In our opinion the settings of SIM matching are not intuitive. Only when we consulted the help, was it clearer to us. When a user uses a device which has no SIM card (e.g. Tablet) disabling SIM matching turns off the red *Security Risk!* warnings and disables alerts on the main screen.

Perhaps it would be better here to rename *Disable SIM matching* to *Hide Security Warnings*.

### *Find*

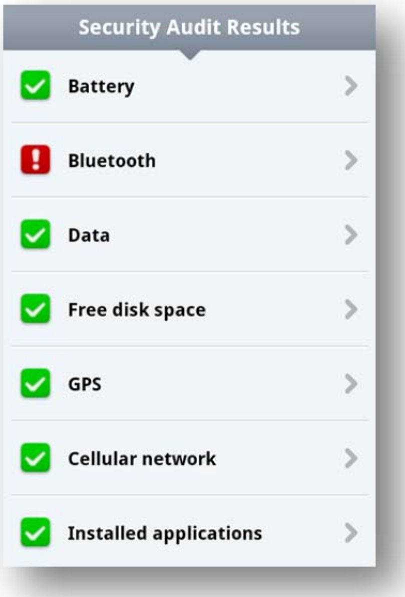
With the aid of the Anti-Theft function ESET Mobile Security makes it possible to locate the phone. Sending an SMS with the command *"ESET find password"* to the device will accomplish this. As a result, the sender will receive an SMS message with a link to Google Maps, and by using it, the user can reach a map on which the position of the phone is indicated.

### *Remote reset*

To use the function of Remote Reset remotely, at least one trusted friend must have been entered in the settings. This friend then has the option of resetting the password.

### Security Audit

The Security audit component checks and displays the status of the mobile phone. It will display all running processes, services and tasks, and shows the actual and target state of device components such as battery, Bluetooth, GPS, memory card, etc.



Security Audit Results

✓ Battery >

! Bluetooth >

✓ Data >

✓ Free disk space >

✓ GPS >

✓ Cellular network >

✓ Installed applications >

### Password

To change their password, the user can use this feature. Also, here the user can determine whether access to areas such as antivirus, anti-spam, anti-theft, and so on is to be password protected.

### Conclusion

ESET Mobile Security offers a comprehensive security product with an anti-spam and anti-theft component.

We should point out that this product was one of few that made data recovery after a remote wipe completely impossible.

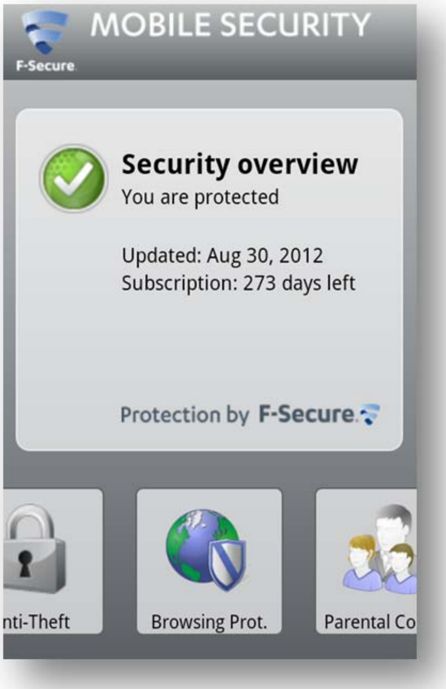
For users who want to operate their smartphone with multiple SIM cards, ESET Mobile Security is a good choice.

Moreover, there is a very good help feature which should answer any questions that come up.

In our opinion, a complexity check of passwords should still be built-in to best protect the user.

## F-Secure Mobile Security

F-Secure Mobile Security includes all the most important protection features of a mobile security suite, such as theft protection, virus protection, and web browsing protection. It is also one of the few products to include a parental control feature.


MOBILE SECURITY
F-Secure

Security overview
You are protected

Updated: Aug 30, 2012
Subscription: 273 days left

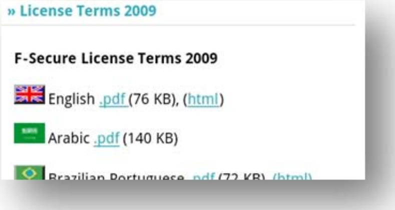
Protection by F-Secure

### Installation

F-Secure Mobile Security (with Parental Control) was downloaded directly from F-Secure's website, and the installation file then started from the file explorer. To make this possible, we had to configure Android to allow non-market apps. The installation was then very straightforward.

### Starting the program

When starting the program, we had to accept the licence agreement, which is exactly the same as it was in 2009.


» License Terms 2009

F-Secure License Terms 2009

English .pdf (76 KB), (html)

Arabic .pdf (140 KB)

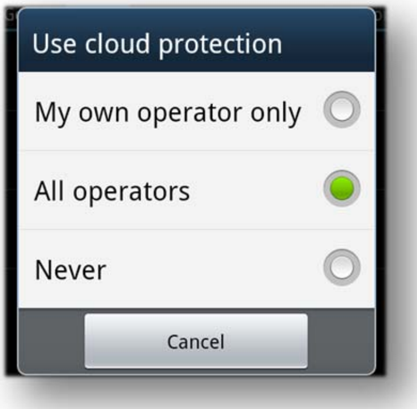
Brazilian Portuguese .pdf (72 KB) (html)

A wizard is then started that guides the user through the configuration process. This allows the use of a free trial version or entering a licence key to use the full version. The wizard also asks the user to enter a 5-digit security code, which is checked for complexity; for example, 12345 was not allowed. An update is also carried out.

At the end of the configuration process, the wizard recommends carrying out a malware scan.

### Virus protection

F-Secure Mobile Security's Virus Protection component allows manual malware scans to be run and automatic scans to be scheduled. Available scan options include checking apps on installation, and whether to scan the SD card.


Use cloud protection

My own operator only ○

All operators ●

Never ○

We particularly liked the fact that F-Secure offers options to prevent additional costs caused by cloud queries when roaming.

The user can choose when to use Cloud Protection for scans. The available options are: always, never, and only when connected to one's own mobile phone provider. The latter option ensures maximum security when "at home", but avoids additional charges when roaming.

### Theft Protection

The theft protection feature ensures that the phone, and the data saved on it, cannot be misused in the event of loss or theft. The relevant commands are sent to the phone by text message. The feature relies on the screen lock features of Android to prevent its being disabled by the thief.

The theft protection component of the software shows its own status, including the activation state of the remote control functions, and the dates of the last lock and last SIM-card change.

### *Find*

Sending a text message with the content“*#LOCATE#[securitycode]*“ allows the location of the phone to be determined remotely. In return, the sender will receive a message containing a link to Google Maps, where the position of the missing phone will be shown.

### *Lock*

The smartphone can be locked by sending the text message *“#LOCK#[securitycode]*“, rendering it inaccessible to unauthorised persons. The android lock screen will be shown on the phone, and the sender will receive a text message confirming the lock, and giving the phone’s co-ordinates.

### *Alarm*

F-Secure Mobile Security allows an alarm to be set off by sending the text message *“#ALARM[securitycode]#[X]”*, whereby X represents the number of times the alarm should be sounded. Unfortunately, there is no information as to how long the alarm sounds each time. In our test, we found that the “alarm” sounds just like a normal ring tone; we feel that a more penetrating sound would be appropriate. F-Secure will in version 8 change the sounds and the volume.

Once sounded, the alarm can be switched off remotely by texting “*#ALARM#[Securitycode]#0*“ to the phone, or locally by unlocking the screen with the appropriate password.

### Wipe

If the user sends a text message with the content “*#WIPE#[Securitycode]*“ to the missing phone, the phone will be returned to factory settings, resulting in all personal data being wiped from it.

### Google account

Resetting the phone to factory settings removes the access data for the Google account, making access to mails or Google Play impossible.

### Data recovery

By using a recovery tool, we were able to restore a majority of the deleted data.

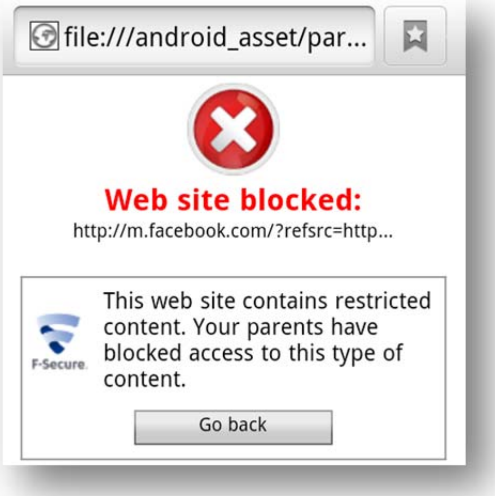
### *Send Location*

The function for determining the phone’s location could be very useful, especially in emergency situations. Selecting this feature from the menu opens up a new text message window with a Google Maps link to the current location. The text message can be sent to any number, and the receiver can instantly see where the user is.

### Browser Protection

The Browser Protection feature prevents malicious websites from being opened with the F-Secure browser. It can be disabled by the user, regardless of current mobile phone provider. Please note that it only works with the F-Secure browser, not the Android browser.

### Parental Control



file:///android_asset/par...

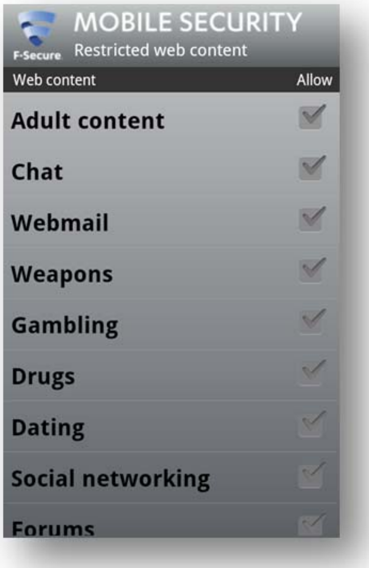
Web site blocked:

http://m.facebook.com/?refsrc=http...

This web site contains restricted content. Your parents have blocked access to this type of content.

This component allows the creation of rules that restrict the content that can be viewed by children, teenagers and even adults by browsing the web. It also places restriction on apps that can be accessed. The pre-configured settings for each age group can be customised.

Pre-defined settings for children block pages relating to e.g. weapons, gambling, and social networks.



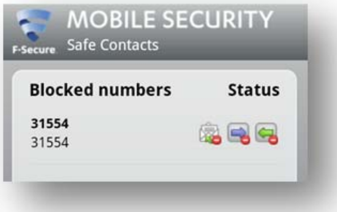
MOBILE SECURITY
F-Secure Restricted web content

| Web content | Allow |
|---|---|
| Adult content | ✓ |
| Chat | ✓ |
| Webmail | ✓ |
| Weapons | ✓ |
| Gambling | ✓ |
| Drugs | ✓ |
| Dating | ✓ |
| Social networking | ✓ |
| Forums | ✓ |

## Secure contacts (Anti-Spam)

Secure Contacts allows blacklisting of undesired contacts. To block calls and texts from certain numbers, these can be entered on a list. This process is somewhat inconvenient, in that it is not possible simply to add numbers from existing contacts. F-Secure will in version 8 include the possibility to add numbers directly from saved contacts and calls.

By default, all incoming calls and texts, and all outgoing calls, are blocked. However, the user can edit or deactivate these rules.



MOBILE SECURITY
F-Secure Safe Contacts

Blocked numbers Status
31554
31554

When a call from a blocked number comes in, the phone rings very briefly, before the number is recognised and blocked. We would prefer the software to react more quickly and block the call without trace.

## Statistics

This supplementary component gives the user a clear overview of the malware/browser protection data.

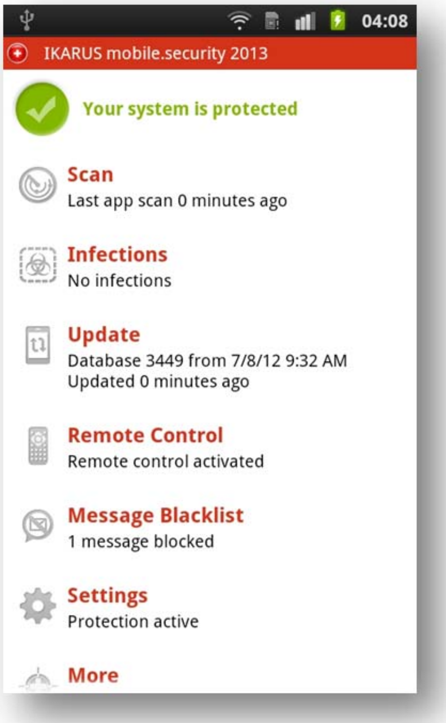
## Conclusion

F-Secure Mobile Security has shown itself to be a well-designed security product. It is particularly suitable for users who want parental controls on a smartphone.

The setup wizard allows anybody to configure the product to their own requirements.

## IKARUS mobile.security

IKARUS mobile.security 2013 is a very clear and easy-to-use security product. It has the most important functions such as antivirus and remote control.



04:08

IKARUS mobile.security 2013

Your system is protected

**Scan**
Last app scan 0 minutes ago

**Infections**
No infections

**Update**
Database 3449 from 7/8/12 9:32 AM
Updated 0 minutes ago

**Remote Control**
Remote control activated

**Message Blacklist**
1 message blocked

**Settings**
Protection active

**More**

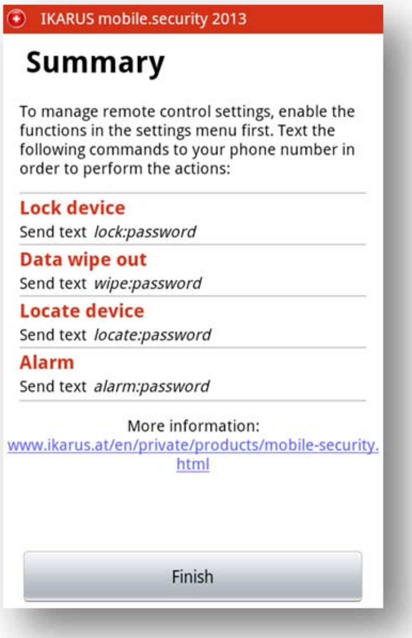
### Installation

IKARUS mobile.security 2013 is available via Google Play. We were able to download and install it easily.

### Starting the program

On starting the program for the first time, IKARUS mobile.security requires the user to enter a 6 – 15 character password for the remote control. The complexity of this is checked, and there must be at least one letter and at least one number.

Having entered a suitable password, we were pleased to note that IKARUS showed us a summary of the most important components. A virus signature update and scan were carried out automatically.



IKARUS mobile.security 2013

**Summary**

To manage remote control settings, enable the functions in the settings menu first. Text the following commands to your phone number in order to perform the actions:

**Lock device**
Send text *lock:password*

**Data wipe out**
Send text *wipe:password*

**Locate device**
Send text *locate:password*

**Alarm**
Send text *alarm:password*

More information:
www.ikarus.at/en/private/products/mobile-security.html

Finish

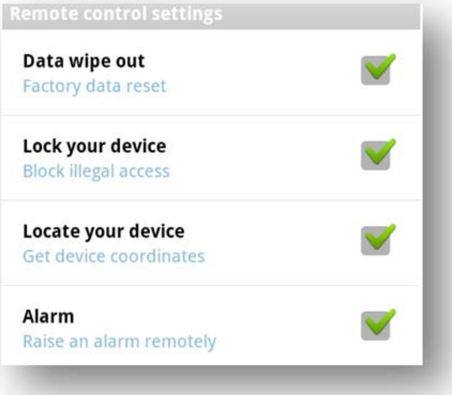
### Scanning

This area allows the user to scan all installed apps, or the entire system.

### Remote Control

Remote Control is IKARUS‘ name for the theft protection features that can be initiated remotely in the event that the phone is lost or stolen. These include wiping, locking, and locating the phone, and sounding an alarm, and are initiated by sending a text message to the lost or stolen phone.

These theft-protection features are deactivated by default and have to be configured by the user before use.



Remote control settings

**Data wipe out** ✓
Factory data reset

**Lock your device** ✓
Block illegal access

**Locate your device** ✓
Get device coordinates

**Alarm** ✓
Raise an alarm remotely

### *Delete Data*

To use this function, the user must register the suite as Device Administrator. We liked the fact that IKARUS only demands this status if the component is activated. With other products, Device Administrator status is demanded during installation, even if none of the active components actually requires it.

Once the feature has been activated, it can be initiated by sending a text message with the content “Delete:[password]”. This resets the phone to factory settings.

#### Google Account

In our test, the reset process successfully deleted the credentials for the Google account, ensuring that there could be no unauthorised access to emails or contacts etc.

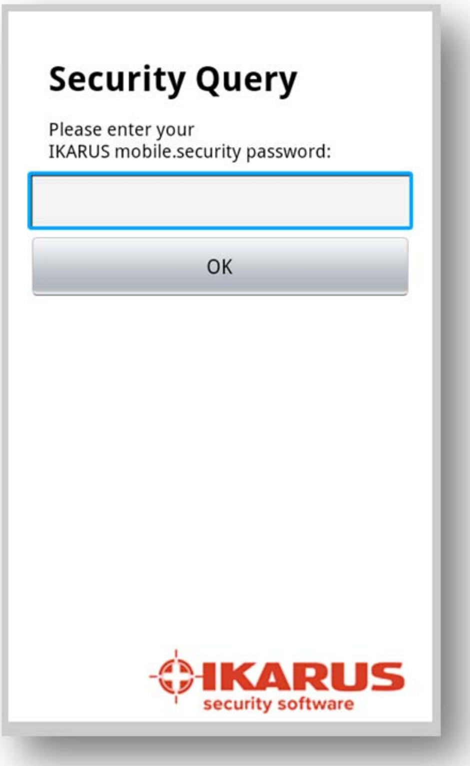
#### Data recovery

We were able to recover the majority of the deleted data on the SD card and internal storage with a recovery tool.

### *Device Lock*

To prevent unauthorised access to the phone if it is lost or stolen, it can be remotely locked by sending a text message with the content “lock:[password]”. A lock screen is shown; this can only be removed by entering the correct password.

When the phone has been locked, it is no longer possible to make emergency phone calls (a contravention of EU law). We would urge IKARUS to rectify this as soon as possible.



Security Query

Please enter your
IKARUS mobile.security password:

### *Locate device*

This function allows the user to locate their lost or stolen phone by sending “locate:[password]” in a text message to the phone. A reply is sent containing a Google Maps link, which will show the phone’s current location.

### *Sound Alarm*

The “Sound Alarm” command causes the phone to emit a loud siren-like sound. Once this intentionally irritating sound has been started, it can only be stopped by entering the correct password.
The alarm is set off by texting “Alarm:[password]“ to the phone.

### SMS Blacklist

IKARUS uses the blacklist concept to prevent unwanted texts. Numbers to be blocked can be entered manually or selected from the address book. An option we liked is the chance to send a text message (freely definable text) back to the unwanted sender.

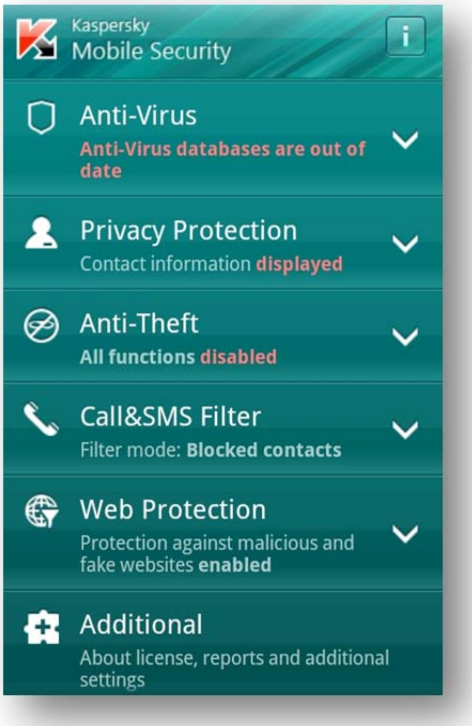
## Conclusion

Ikarus mobile.security 2013 contains the essential functions of a mobile security suite. The user interface is very clearly laid out, and all users should find it intuitive to use.

We felt that for the price charged, it would be reasonable to expect more functionality. We would expect the ability to make emergency phone calls even when the phone is locked.

## Kaspersky Mobile Security

This year's Kaspersky product once again includes the most important security components, such as Anti-Virus and Anti-Theft, but also has a new feature: Web Protection.



Kaspersky Mobile Security

Anti-Virus
Anti-Virus databases are out of date

Privacy Protection
Contact information displayed

Anti-Theft
All functions disabled

Call&SMS Filter
Filter mode: Blocked contacts

Web Protection
Protection against malicious and fake websites enabled

Additional
About license, reports and additional settings

### Installation

We downloaded Kaspersky Mobile Security directly from the manufacturer's website, and then ran the installation file using the file explorer.

### Starting the program

When Kaspersky Mobile Security is started for the first time, a welcome message appears, informing the user of the most important components of the suite. The user is then given the choice of entering a licence key to activate the full version, or using the trial version.

The next step is to set the program as Device Administrator, and enter a "Secret Code", which will be checked for complexity.

There is then the opportunity to enter an email address for reminders, in case the Secret Code is forgotten.

We noticed in our test that this email address is not verified. In the event that the user makes a mistake when entering the address, it will not be possible to reset the Secret Code. This could be avoided if the user had to verify the email address used by replying to a confirmation email sent to the address entered. We feel this is especially important as we were not able to change the email address later.

Neither an update nor a malware scan was carried out automatically at the first start, although the program does inform the user that the virus definitions are out of date.

### Anti-Virus

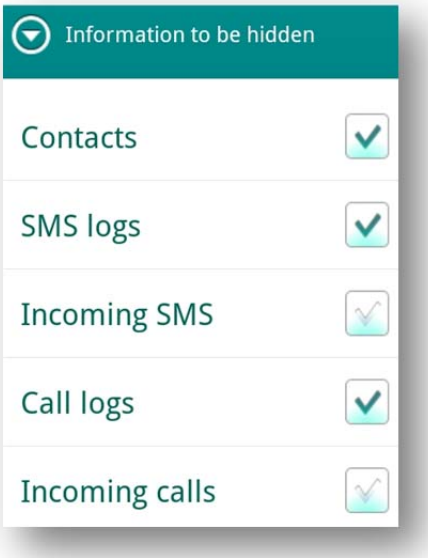
The real-time protection in Kaspersky Mobile Security is activated by default. The user can start a manual update or malware scan from this menu item, with a choice of Full, Folder or Memory scans.
There is a wide choice of configuration options, such as the action to be taken on malware discovery, which file types to scan, and when to run scans.

This year, a new component called *"Cloud Security Scan"* has been introduced, which scans apps with the cloud-based Kaspersky Security Network.

### Privacy Protection

Privacy Protection allows the user to prevent unauthorised transmission of confidential data such as contacts, call and text logs, text messages, by hiding it. This component is not activated by default.

Telephone numbers to be blocked can be entered directly or selected from the address book.



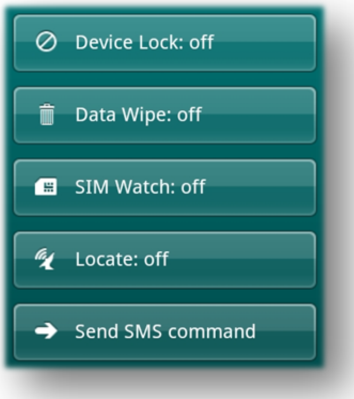
Information to be hidden

- Contacts ☑
- SMS logs ☑
- Incoming SMS ☑
- Call logs ☑
- Incoming calls ☑

Sending a text message with the content “hide:[code]“ allows the private data to be hidden remotely. We were pleased to see that the sender receives a confirmation email in return.

## Anti-Theft

When it comes to theft protection, Kaspersky Mobile Security has features such as Device Lock, Data Wipe, SIM Watch and Locate. These are not activated by default, but can be switched on individually.



- Device Lock: off
- Data Wipe: off
- SIM Watch: off
- Locate: off
- Send SMS command

## *Device Lock*

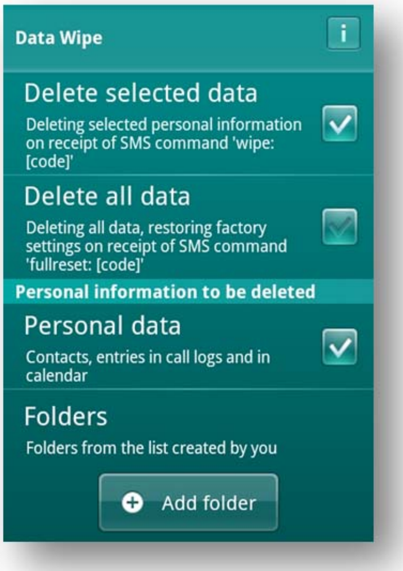
Sending a text message to the phone with the content “lock:[code]” locks the phone. It can be unlocked by entering the Secret Code (using the Recovery of Secret Code routine if necessary).

In our test, we used the Recovery Routine a number of times. It occurred to us that we received the same Recovery Code each time. When this had been entered, the Secret Code was displayed in clear text.

## *Data Wipe*

Kaspersky Mobile Security offers two different means of using the Data Wipe feature. The first, using the command “wipe:[code]”, deletes the user’s private data plus any additional folders chosen by the user. Kaspersky’s definition of private data includes personal files, contacts, calendar entries and the call log, but not emails – something we find curious.

The second wipe option uses the command “fullreset:[code]”, and resets the phone to factory settings.



Data Wipe

Delete selected data ☑
Deleting selected personal information on receipt of SMS command 'wipe:[code]'

Delete all data ☑
Deleting all data, restoring factory settings on receipt of SMS command 'fullreset: [code]'

Personal information to be deleted

Personal data ☑
Contacts, entries in call logs and in calendar

Folders
Folders from the list created by you

In the settings of Data Wipe, Kaspersky claims that all data will be deleted by the Full Reset process.

When we tested the Full Reset function, however, we found that the data on the internal storage and on the SD card was NOT wiped. Only if these storage areas are manually added to the list of items to be wiped does the Full Reset process do what it claims to do. We feel that Kaspersky should make this clear to the user.

The same is true of the Wipe command: only if the internal and external storage areas are deliberately added does the wipe process actually delete the data on them.

### Google account

The Full Reset process successfully wiped the credentials for the Google account and made access to the account from the phone impossible.

The Wipe command deletes the Google account credentials, but does not reset the phone, meaning that phone can still be remotely controlled using Kaspersky Mobile Security.

### Data recovery

We were able to recover the great majority of the "wiped" data on both the external and internal storage areas with the assistance of a recovery tool.

### *SIM Watch*

If the SIM Watch component is activated, the user will be informed of any change of SIM card in the device. This is done by sending the telephone number of the new card to a pre-defined phone number/email address.

We especially liked the fact that it is possible to configure an automatic lock, with a freely editable message displayed, in the event of the SIM card being changed.

### *Locate*

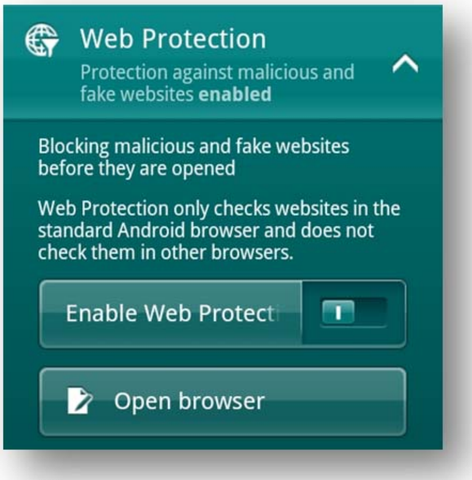
The command "locate:[code]" as a text message sent to the phone will cause its current location (GPS co-ordinates) to be texted to the sender's phone, and sent as an email to the address registered during the activation process.

## Call&SMS Filter

The Call&SMS Filter uses blacklists and whitelists, i.e. lists of numbers to block or allow, respectively. Anonymous calls, i.e. those with the caller's number withheld, can be blocked.

## Web Protection

Web Protection is activated by default, and blocks risky or fake websites before they can be opened. This function only works with the standard Android browser.



Web Protection

Protection against malicious and fake websites **enabled**

Blocking malicious and fake websites before they are opened

Web Protection only checks websites in the standard Android browser and does not check them in other browsers.

## Conclusion

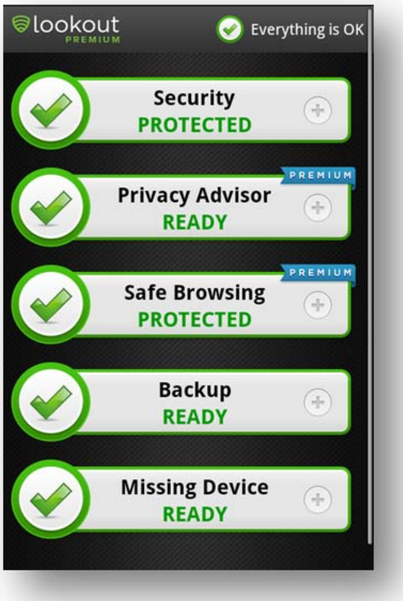
Kaspersky Mobile Security is a comprehensive security product. It is one of very few programs to protect the user's private data, which it can do by hiding contacts, texts and call histories.

The individual components are clearly explained and come with a detailed help function.

We feel that the email address used in the recovery of the Secret Code should require verification, in order to guard against typing errors. We would also like the ability to change it later.

## Lookout PREMIUM

Lookout PREMIUM provides the user with modern security features such as anti-spam, surfing protection and theft protection. There is also a backup function, which can be automated.



### Installation

The free version of Lookout can be easily downloaded and installed from Google Play. There is then the option of testing the Premium version free of charge for two weeks. Once the trial period has expired, the software automatically downgrades itself to the free version.

The configuration instructions are very clear and suitable for all users.

Accessing the web interface[7] in order to access backed up data, or to locate the phone if it has been lost, requires the user to create a new account or enter existing credentials.

### Starting the program

When Lookout PREMIUM is started for the first time, it will scan the mobile phone for malware.

Unfortunately we were not able to find the update status anywhere.

### Security

Under this menu item can be found information about the last malware scan, and a button to start a new scan.

The virus scanner can be configured in the configuration menu. The user can then choose from options to turn the security module on or off, enabling File System Monitoring, or selecting the frequency of Scan Schedule.

### App-Adviser

The App-Adviser scans all installed apps on the device, and lists them with their critical access permissions, such as contacts, texts and location. Clicking on the App Info and Options button takes the user to the Android menu for stopping and uninstalling apps.

### Safe Surfing

Lookout protects the user against unsafe websites while surfing with the standard Android browser. There are no configuration options available.

### Backup

The Backup feature saves user data onto a Lookout server. The data is backed up in the form of snapshots, which can be combined to form a complete backup of data over a period of time.

Backup can save contacts, call history and pictures, although the latter is not saved by default due to the high battery usage required. As with the malware scan, the backup process can be automated according to a schedule.

In our test, pictures and call logs were saved as expected. With contacts, however, only those items that synchronise with the Google account were backed up; local contacts were not included.

Restoring data is controlled using Lookout’s web interface.

[7] http://mylookout.com

## Device Location

Device Location is Lookout's terminology for theft protection. It can be optimised using the Extended Protection setting, which registers the program as device administrator. No other configuration options are available.

The anti-theft features include device location, alarm signal, locking and wiping the phone. Control is via the web interface; Lookout intentionally does not offer the ability to use text messages for this purpose in order to keep its users from being exposed to potential vulnerabilities.

### *Locate*

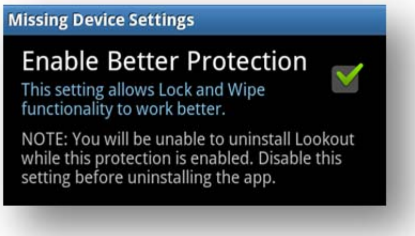
Once the command to locate the phone has been sent from the web console, the position of the device will be shown on a Google Maps map in just a few seconds. The service cannot be deactivated.

### *Alarm*

This feature emits a loud warning sound, even if the volume setting on the phone has been set to silent. The sound can be deactivated without entering a PIN, unless the phone has already been locked.

### *Lock*

This locks the mobile phone, making access for unauthorised persons impossible – at least in theory. If the Extended Protection (Device Administrator status) has not been activated, the phone can be unlocked by pressing the emergency call button, and then Home (no PIN required). The relevant settings page of Lookout informs the user that the Extended Protection improves the remote lock function, but does not make any reference to this problem. Lookout is currently working on a fix which should be released in the next version.



Missing Device Settings

Enable Better Protection ✓

This setting allows Lock and Wipe functionality to work better.

NOTE: You will be unable to uninstall Lookout while this protection is enabled. Disable this setting before uninstalling the app.

### *Wipe*

The Wipe function removes all personal data (contacts, photos, Google account credentials etc.).

Once again, the relevance of the Extended Protection setting has not been made clear in its description. After many test runs we concluded that if Extended Protection is deactivated, all personal data will be deleted by the Wipe function. However, if Extended Protection is switched on when the Wipe command is given, the phone will be reset to factory settings, removing all installed apps, including Lookout, which will then have to be reinstalled from scratch.

Lookout itself appears not to be aware of this procedure. If the Wipe command is given without Extended Protection having been activated, the Lookout software will remain installed on the phone and active. However, the web interface will inform the user that the phone has been reset to factory settings, and that it will be necessary to reinstall the Lookout software.
Lookout will improve the issues mentioned above in an upcoming update.

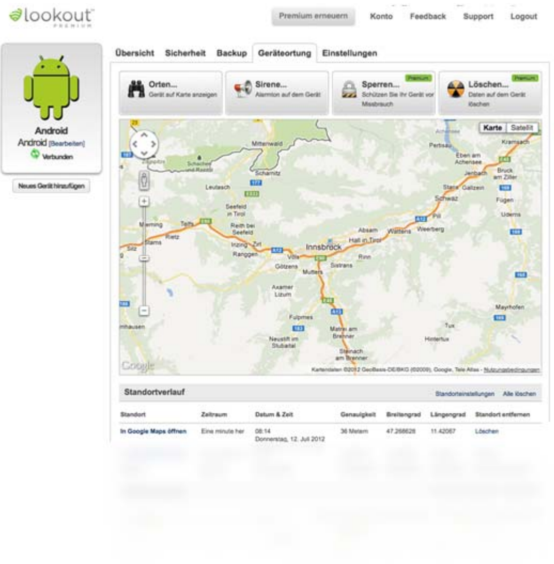
### Google Account

Access to the Google account is successfully removed by the Wipe command, regardless of the status of the Extended Protection. With EP off, the password is deleted, along with other personal data; with EP off, the phone is reset, removing all data, configuration and apps.

### Data recovery

In both cases, we were able to recover much of the deleted data, as the storage was neither overwritten nor properly reformatted.

## Web interface



| Standort | Zeitraum | Datum & Zeit | Genauigkeit | Breitengrad | Längengrad | Standort entfernen |
|---|---|---|---|---|---|---|
| In Google Maps öffnen | Eine minute her | 08:14<br>Donnerstag, 12. Juli 2012 | 36 Metern | 47.268628 | 11.42067 | Löschen |

The web interface is very well structured and easy to use. It provides the only means of controlling the remote functions (locate, alarm, lock and wipe) and can also be used to initiate the backup process.

## Conclusion

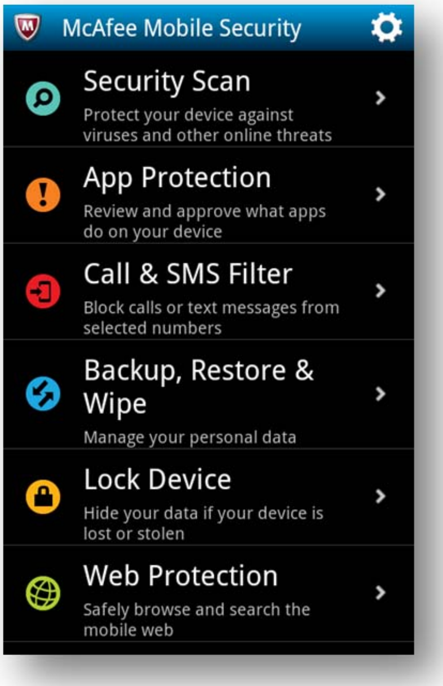
Lookout PREMIUM provides a very good product description when the program is first started. This informs the user clearly about the integrated functionality.

For users who want an integrated backup function, Lookout PREMIUM could be an option.

Areas that need to be improved are the weaknesses of the Wipe function (as mentioned above), inadequate description of individual configuration options, and the backup of all contacts.

## McAfee Mobile Security

McAfee Mobile Security is a complete security packet with the most important functions, such as theft protection, malware and surfing protection. It also includes a well-engineered backup function that can be operated via a web interface.


McAfee Mobile Security

Security Scan
Protect your device against viruses and other online threats

App Protection
Review and approve what apps do on your device

Call & SMS Filter
Block calls or text messages from selected numbers

Backup, Restore & Wipe
Manage your personal data

Lock Device
Hide your data if your device is lost or stolen

Web Protection
Safely browse and search the mobile web

### Installation

McAfee Mobile Security can be downloaded and installed via Google Play. After accepting the licence agreement, the user is taken through a step-by-step process of creating a McAfee account. An email address and a PIN code have to be entered. A welcome message, which gives a good overview of the product, is sent to this address at the end of the process.

If there is no SIM card in the phone at the time of installation, McAfee Mobile Security cannot be started, as it is not possible to register the device.

### Starting the program

When the program is started, a home screen is shown, on which all the components of the suite are listed. Additionally, any possible problems are shown at the lower edge of the screen. There is a reminder to register the program as device administrator, activate GPS, and to set up the screen lock and automatic backup functions. There is no advice regarding running a malware scan.

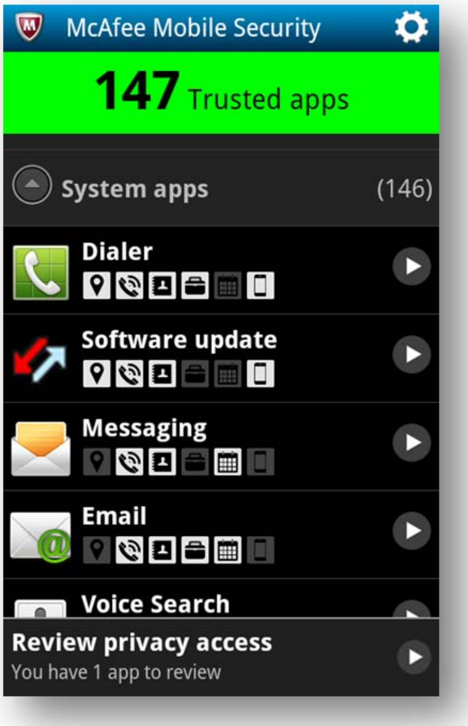
### Security Scan

The Security Scan component protects the device from malware and other threats. Updates and scans can be started manually. Real-time protection, automatic updates and scheduled scanning are activated by default.

### App Protection

App Protection checks the activities of the installed apps. After a short introduction and explanation of the symbols, all installed apps are scanned. A very clearly laid-out list shows all the apps and their access permissions. Clicking on Show App Details takes the user to the Android menu from which the app can be stopped or uninstalled.

An additional list can be shown, which itemises all apps according to their access permissions. For example, the user can configure the list to show all apps that are allowed to access the device's location information.


McAfee Mobile Security

147 Trusted apps

System apps (146)

Dialer

Software update

Messaging

Email

Voice Search

Review privacy access
You have 1 app to review

### Call & SMS Filter

The Call and SMS Filter uses whitelisting and blacklisting to block ingoing and outgoing calls and text messages. Entries can be made to both lists from contact information, call logs, text message logs, and manual entry.

If a contact should appear in both the blacklist and the whitelist, the blacklist takes priority, meaning that the call is blocked. We suggest that McAfee should either warn that a contact has been put in both lists, or prevent this from happening.

When a call is received from a blacklisted number, the phone rings and displays the number for a fraction of a second before McAfee intervenes. We would prefer to see a quicker reaction, blocking the call entirely.

Text messages can also be blocked on the basis of freely definable key words. For example, any text containing the word "lottery" could be blocked.

### Backing up, restoring, and wiping.

Backing Up, Restoring & Wiping offers a comprehensive and easy-to-use backup solution. Backed-up data is stored on a McAfee server and can be viewed using a web browser.

#### *Backing up*

The user selects what to back up by tapping appropriate menu items. Text messages, call histories, contacts and media (photos and videos) can be uploaded. McAfee also offers automated backups, carried out according to a schedule.

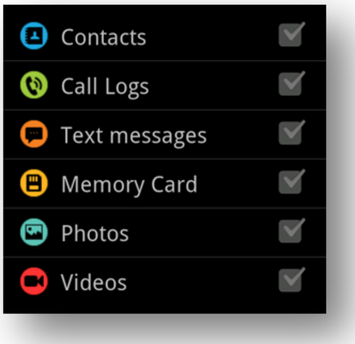
The help function explains that photos and videos are not backed up automatically, but can be saved by running an appropriate manual backup.

#### *Restore*

The Restore function allows text messages and contacts to be restored. Restoring backed up photos and videos cannot be done through the phone itself, but is possible using the web interface.

#### *Wipe*

Contacts, call lists, text messages, contents of the SD card, photos and videos can be deleted directly from the phone using McAfee Mobile Security.



The items to be deleted can be selected individually.

In our test, all the selected items were successfully deleted.

### Google Account

The Google account credentials were not deleted in our wipe test. This means that in the event of account synchronisation taking place, all Google account data such as contacts will be completely deleted from the server as well as from the phone. Equally, if a thief does not carry out synchronisation, they will have access to all the Google account data, unless the phone's owner manually resets the Google account password through Google's web interface. Without the password being reset, the thief would also be able to purchase items from the Google Play store, the costs for which would be charged to the legitimate owner.

We feel that McAfee must improve this situation, in order to protect the owner effectively. McAfee responded that they will enhance this in a future release.

### Data recovery after wipe

In our test, we found it was possible to recover much of the “wiped” data from both the internal storage and the SD card.

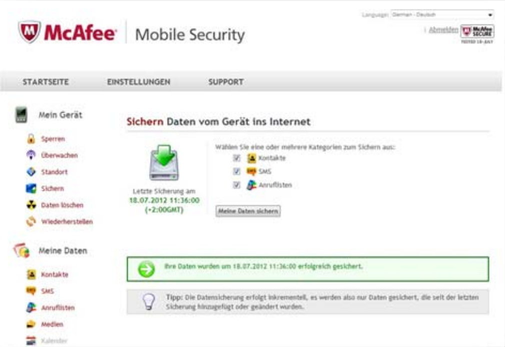
## Device lock

This function allows the device to be locked, using the PIN code entered during installation.

## Web Protection

Web Protection is activated by default and protects the user against malicious websites when using the standard Android browser.

## Web interface



Sichern Daten vom Gerät ins Internet

Letzte Sicherung am 18.07.2012 11:36:00 (+2:00GMT)

Wählen Sie eine oder mehrere Kategorien zum Sichern aus:

☑ Kontakte
☑ SMS
☑ Anruflisten

Ihre Daten wurden um 18.07.2012 11:36:00 erfolgreich gesichert.

Tipp: Die Datensicherung erfolgt inkrementell, es werden also nur Daten gesichert, die seit der letzten Sicherung hinzugefügt oder geändert wurden.

The web interface[8] gives the user the ability to control the anti-theft functions remotely. Possible actions include locking the phone, monitoring the SIM card (in case it is replaced), determining the phone’s location, backing up and then wiping data from the phone. The web interface can also be used to access the backed-up data. It should be noted that it is the only means of remotely controlling the security suite functions; no text-message commands are possible.

In our test, we used the same email address as last year when setting up McAfee Mobile Security, but with a different phone number. When we logged on to the web interface, we found that the account was still linked to the old mobile phone. Consequently we were shown an expired licence and obsolete data. It was only when we registered the new phone number that up-to-date information relating to our current device was shown.

We suggest that McAfee should point out that such an anomaly can occur, or ideally allow the web interface to administer multiple devices.

### *Lock*

The device can be locked and unlocked from the web interface. The user has the option of sounding an alarm when the phone is locked.

### *Guard*

The Guard function displays the number of the currently fitted SIM card. If the card is changed, the last few digits of the new number will be displayed, and the phone automatically locked.

### *Location*

McAfee is one of very few manufacturers to offer continuous surveillance of the phone’s location, as opposed to a one-off snapshot. Location data can be recorded for up to 6 hours and displayed on a map.

### *Wipe using the web interface*

When wiping data using the web interface, the user is able to select items to be wiped in exactly the same way as when using the using the phone’s own interface locally.

## Conclusion

McAfee Mobile Security impressed us with its very well thought-out user interface and web console. Every function is fully explained in the comprehensive help feature.

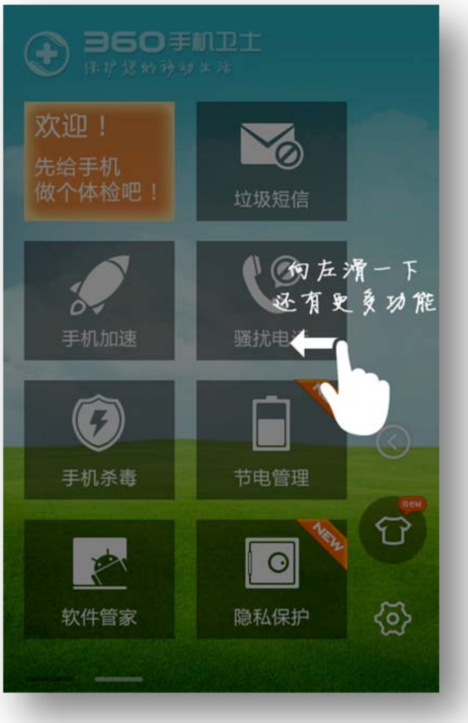
As well as the normal security features, McAfee’s suite includes backup function.

In this year’s test, we once again encountered the problem with the Google account credentials not being removed by the wipe process, something we feel McAfee should rectify urgently. As it is impossible to register the suite unless a SIM card is in place, the suite is totally unsuitable for a device being used without a SIM card.

[8] https://www.mcafeemobilesecurity.com/

## Qihoo 360 Mobilesafe

Qihoo MobileSafe is a free security solution with a wide range of features and the possibility to add even more. Most of the extended features can only be installed if the user has allowed the installation of non-Google-Play apps in the settings.



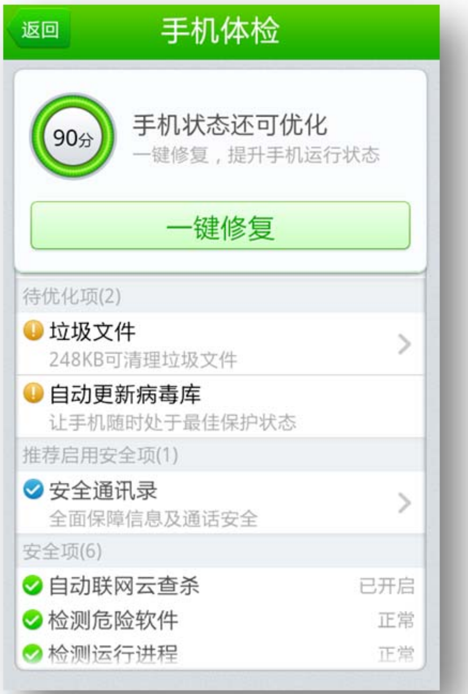
The suite has so far only been available in Chinese language. More Android devices are activated every day in China than in the USA. For this reason, we are especially pleased to include this product from Beijing.

### Installation

The installation file was downloaded from Google Play. As an alternative, Qihoo Mobilesafe can be downloaded directly from the manufacturer's website.

### Starting the program

When the program is started for the first time, the licence agreement and privacy notice have to be accepted. Following this, the user is shown basic usage instructions. Instructions marked in orange encourage the user to run a device health check. We followed this advice, and our smartphone received a total of 90 points in the health check.



手机状态还可优化

一键修复，提升手机运行状态

待优化项(2)

垃圾文件 ›
248KB可清理垃圾文件

自动更新病毒库
让手机随时处于最佳保护状态

推荐启用安全项(1)

安全通讯录 ›
全面保障信息及通话安全

安全项(6)

| | |
|---|---|
| 自动联网云查杀 | 已开启 |
| 检测危险软件 | 正常 |
| 检测运行进程 | 正常 |

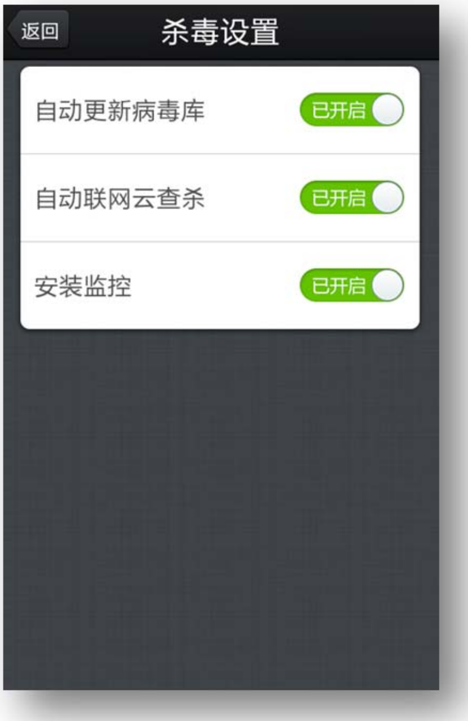
The suite found fault with the Google Play store, which it deemed to be 244 KB of wasted storage, and the fact that the automatic update of virus definitions was deactivated. The "Repair With One Click" button removed both reported issues giving a further 10 points, making a total of 100 and reaching "Green" in the device health status. No mention was made in the checkup of the unconfigured theft protection module.

Carrying out the health check again then (surprisingly) only produced a score of 92 points. 25 running processes were criticised, and the program asked us to click the "Repair With One Click" button again, to clean up the memory. The health check appears to be actually a form of security training for the user. Running the check on different devices with different numbers of processes running managed to produce the same number of points in the checkup.

After the first checkup the virus signatures were up to date, and the automatic update switched on.

## Mobile AntiVirus

The Mobile Anti-Virus button takes the user to the scan menu. Qihoo offers a complete scan or a quick scan. The settings here allow the following to be activated or deactivated: automatic definition update, automatic cloud scan, and installation guard. The latter feature is activated by default.



杀毒设置

自动更新病毒库 已开启

自动联网云查杀 已开启

安装监控 已开启

The quick scan took two seconds to run and found 320 "programs". The complete scan took 10 seconds.

## Optional AV Add-On

Qihoo offers an additional malware removal tool for removing the "Kung Fu Trojan", and a new proactive protection module.

The so-called proactive protection module is still marked as a beta version. After installing it, we had to authorise Root permissions for 360Mobilesafe again.

## Anti theft

This component is deactivated by default. When activating it, the user has to enter a 6-12 digit PIN code, and a trusted phone number, to be informed in the event that the SIM card is changed.

To use the anti-theft functions, Mobilesafe users have to send text messages to the lost or stolen phone. This worked correctly in our test.

Most security software manufacturers use English text commands, regardless of the language of the interface. Qihoo, on the other hand, uses Chines commands rendered in the Latin alphabet: delete (shanchu 删除), locate (weizhi 位置), scream (baojing 报警), lock (suoding 锁定) antitheft (警报) etc.

The text command "*fangdao#password*" allows the phone to be located and locked, whilst sounding an alarm.

### *SIM-Watch*

This sends a contact of your choice a text message to say that the SIM card has been changed. The wording of the text can be defined during setup.

### *Locate*

Sending „*weizhi#password*“ as a text message can find the location of the phone. The sending phone receives a message back with a description of the location in words, and a map from Qihoo Maps Service, with the point marked.

### *Alarm*

This function allows the user to sound the alarm on the smartphone, without locking it. The alarm only goes off for a few minutes. The command to be sent by text message is "*jingbao#password**".

### *Lock*

The command "*suoding#password*“ locks the phone to prevent unauthorised access. It can then only be unlocked by entering the correct password. According to Qihoo's documentation, entering a false password takes a photo of the suspected miscreant.

### *Delete*

The command *"shanchu#password*" is supposed to delete private data, including text messages, contacts, call log, and all personal data files. The device is not reset to factory settings, meaning that the theft protection software continues to run. In our test, the contacts and text messages were successfully deleted on all devices. However, on one device the call log survived, even though 360Mobilesafe had confirmed successful deletion in a text message.

### Google Account

The password for the Google account was successfully deleted, blocking access to mails etc.

There was no point in attempting data recovery in our test, as neither the internal nor the external storage had been wiped.

### Password

The text command *"mima#password*" allows the security password to be changed.

### Privacy protection

Qihoo Mobilesafe offers a variety of functions to protect the user's privacy.

### Password protection

The user can set a password for the 360Mobilesafe program itself, meaning it cannot be opened without the password being entered.

### Privacy Guard

The privacy guard feature is explained to the user as a safe, which password protects text messages from specified numbers, selected photos, videos and other files. It should be noted that even the simplest passwords such as "12345" are accepted by Mobilesafe. In order to protect the photos, videos and other files, another supplementary program has to be installed. Again, this is a non-Google-Play app.

After the installation, the user must accept another licence agreement, and once again decide whether to send product feedback to Qihoo.

The Safe password should have between 1 and 12 characters. We tried using simply "1" as a password, and this was accepted. After that, a security question can be entered again.

If the user adds e.g. certain photos to the Safe, the photos can only be seen in the private album in the safe, and not in the general gallery.

The Safe can also be used to password protect individual apps. Protected apps can only be started by entering the password.

Even after we uninstalled and reinstalled Privacy Guard, we were unable to access the program without entering the password we had set up during the first installation.

### *Anti-eavesdropping*

This feature is activated by default, and is intended to protect against your phone calls being bugged.

### Nuisance calls and text spam

Qihoo has integrated functions to prevent the user being pestered by nuisance calls and text spam. As well as the usual blacklist and whitelist, there is a feature that allows the user to send spam texts to Qihoo. Again this has to be installed as a supplementary program. The ability to register the spam texts with Qihoo provides the user with a certain sense of satisfaction (tester's verdict: ☺). During the test, using a Unicom Post-Paid SIM card, several spam SMS were received and correctly handled.

### The "Mobile Phone Accelerator"

A few clicks in the Mobile Phone Accelerator cause running apps to close and unused memory to be made free. "One Click Optimisation" makes it quick and easy for users to run a simple optimisation procedure.

### Energy Manager

The 360 "Energy-Saving King" is another supplementary app which has to be installed separately. Again it is a non-Google-Play app. It is supposed to give the user more control over their phone's power consumption.

### Software Manager

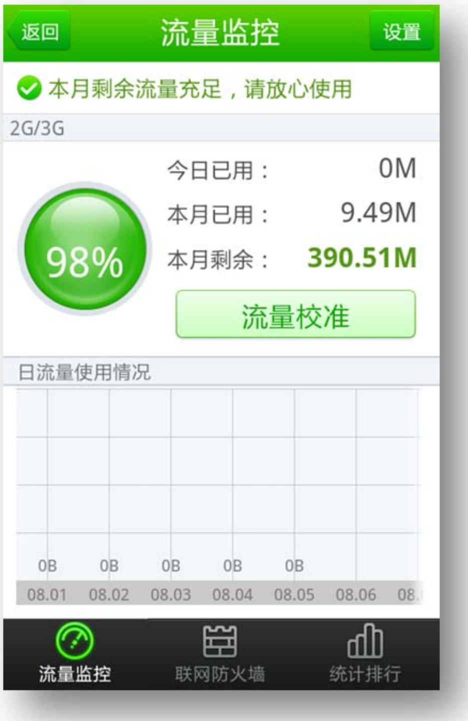
Here Qihoo offers management of application updates and deinstallation, installation packages, a feature to move apps from the internal storage to the SD card or vice-versa, and a detailed system overview.

### Secure Backup

This feature allows the backup and restore of contacts, all texts (including password protected ones) and the 360MobileSafe settings. The user must register for an account or use an existing one. The username is the mobile phone number. The backup log can be restored or deleted. Backed-up data can be stored on the SD card.

### Traffic Manager

Qihoo Mobilesafe's Traffic Manager shows the daily and monthly data traffic. Additionally, the monthly data limit set by the mobile phone provider can be entered, and the amount that has been used up is shown in the notification menu. By means of text messaging to the Chinese mobile-phone service provider, the feature was able to find both the monthly limit and the amount of data already used. The intervals at which the text messages are sent to the service provider can be configured.



返回 流量监控 设置

本月剩余流量充足，请放心使用

2G/3G

今日已用： 0M
本月已用： 9.49M
本月剩余： 390.51M

98%

流量校准

日流量使用情况

流量监控 联网防火墙 统计排行

### *Firewall*

The firewall, an integral part of the suite, lists installled apps. It is not possible to make any changes. There is a message that the component does not have Root permissions.

### *Other tools*

Under this menu item, Qihoo offers functions such as file management and a system test. Network settings can be imported and exported. The account balance can be obtained from Chinese service providers via text message. Although a similar service was included with our Post-Paid Unicom SIM card, we found that 360Mobilesafe's version was more user-friendly.

It is possible to directly check which regional service provider a Chinese mobile phone number belongs to. In our test, numbers from various different provinces were correctly identified. This function serves as a quick plausibility check for unknown callers.

The last menu item contains useful items for Chinese users, with numbers to call to order train and plane tickets, hotel reservations, banks, insurance companies and telephone service providers.

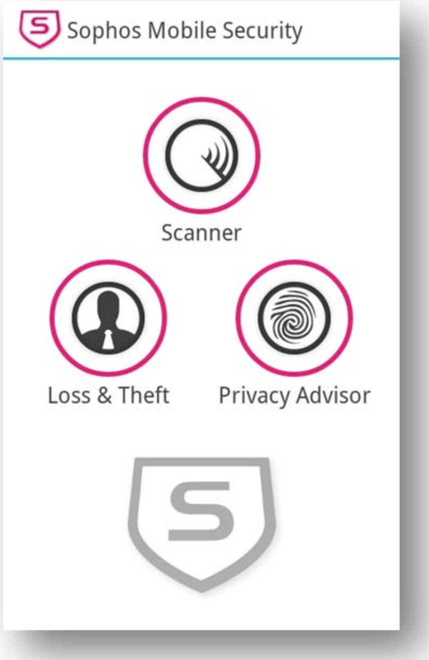
## Conclusion

Qihoo MobileSafe has shown itself to be a very comprehensive product. As well as security components, the suite contains optimisation tools and functions to help users in everyday situations in China. The integrated Traffic Manager, which can be synchronised with the service provider’s usage data, is an interesting addition.

The Wipe function should also delete the contents of the SD card, in order to provide the best possible protection for the user. A password of ONE character should not be allowed, for security reasons. Chinese businessmen and tourists can be seen all over the world; for this reason, the location function of the theft protection should work optimally even outside of mainland China.

## Sophos Mobile Security

Sophos Mobile Security is a free security product, which has been kept very simple and clean in its design. Its functionality is limited to a malware scanner, theft protection, and listing of access rights for all other apps on the phone.



### Installation

We were able to download and install Sophos Mobile Security from Google Play without any difficulty. The application starts immediately after the licence agreement is accepted.

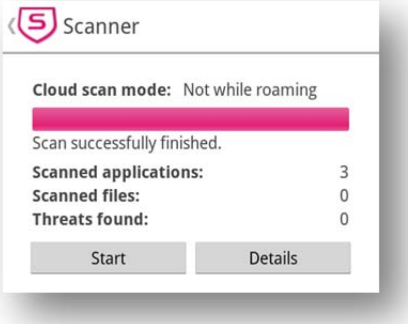
### Starting the program

On starting the program for the first time, a very simple and clear menu is shown. Unfortunately, the anti-malware component neither initiates a scans after installation automatically, nor there is nothing to inform the user that the *Loss & Theft* component is deactivated. In the next version of Sophos Mobile Security, an initial scan after installation will take place and the user will be informed about the deactivated components.

A possible means of informing the user of an item's status would be to replace the pink ring with a green one for any components that are up-to-date and active.

### Scanner

To check the smartphone for malware, Sophos provides the Scanner component. This has a very clear and simple interface. In the settings it is possible to configure Cloud Scan Mode, scanning of apps during their installation, scanning of SD cards, and scanning of system application.



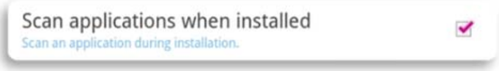
**Cloud scan mode:** Not while roaming

Scan successfully finished.

| | |
|---|---|
| **Scanned applications:** | 3 |
| **Scanned files:** | 0 |
| **Threats found:** | 0 |

We especially liked the ability to deactivate Cloud Scan Mode when roaming, in order to avoid a hefty bill from the mobile phone service provider.

We were a little confused by the disparity between the menu item "Scan application **after** installation" and its description (effectively a subtitle), "Scan application **during** installation". This disparity will be corrected with the next release.



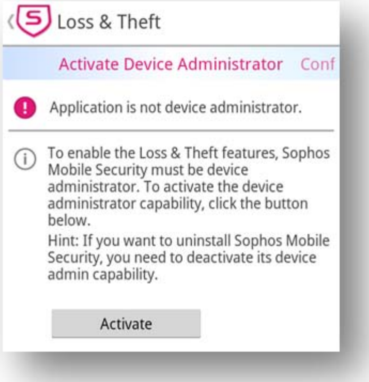
Scan applications when installed ☑

Scan an application during installation.

Whilst this does not have any bearing on the effectiveness of the scan, it leads to uncertainty on the part of the user, and we feel it should be corrected.

### Loss & Theft

This feature is deactivated by default. Its configuration is very simple, as the user is assisted by clear and simple instructions. To arrive at the configuration steps, however, the user has to swipe the screen, which is not immediately apparent.


Loss & Theft

Activate Device Administrator Conf

Application is not device administrator.

To enable the Loss & Theft features, Sophos Mobile Security must be device administrator. To activate the device administrator capability, click the button below.

Hint: If you want to uninstall Sophos Mobile Security, you need to deactivate its device admin capability.

Activate

The first step is to activate the device administrator. Next, the Android screen lock has to be configured and the location service started. An SMS password then has to be defined, consisting of at least 4 alphanumeric characters. Finally, up to five telephone numbers are entered, which are allowed to control the phone remotely if necessary.

Sophos Mobile Security informs the user in the event that any configuration items have not been successfully completed.

*Loss & Theft* functions are limited to locating and locking the phone. These are initiated by sending a text message to the phone, whereby the phone number used to send the message must have been registered in the setup process as described previously.

We are not convinced that this is a sensible solution, as there is no record of the numbers that have been used other than in the phone itself. For the Loss & Theft functions, to be useful, the user must make a record of the phone numbers entered and their owners; using all 5 would make sense, in case some of the friends change mobile phone providers and get new numbers as a result.

### *Lock*

When a text message with the content “lock [password]“ has been sent to the phone, it will be locked with the standard Android lock screen. The message sender will receive a message to confirm that the remote phone has been successfully locked.

### *Locate*

Sending a text message with the content *“locate <password>”* to the phone allows it to be located. This works very quickly and reliably. The phone that sent the locate command receives a text message by return that contains the co-ordinates of the phone, along with a link to Google Maps showing these on the map.

In our test, we noticed that it is not necessary to enter a password in order to deactivate the theft protection features, or to change the SMS password. Sophos relies on Android’s own lock function, which can be configured (optionally) whilst setting up the suite.

## Privacy Advisor

This feature lists all apps on the phone which require special permissions. This includes apps which may induce data transfer costs, cause data protection problems, or use the Internet.

## Conclusion

Sophos Mobile Security is an easy-to-use product with limited functionality. Thanks to the excellent instructions, it should be straightforward to configure it appropriately.

Unfortunately, the suite does not include a remote Wipe function, meaning that personal data cannot be erased in the event of the phone being lost or stolen. Sophos is already working on adding in version 8 additional components like e.g. Remote-Wipe, Remote-Alarm, Security-Advisor, detection of potentially unwanted apps, etc.

## Trend Micro Mobile Security

Mobile Security by Trend Micro stands out with its appealing design and consistent user interface. Functionality has also reached a high level. For example, as well as standard functions such as theft protection, the suite also includes a parental control feature.

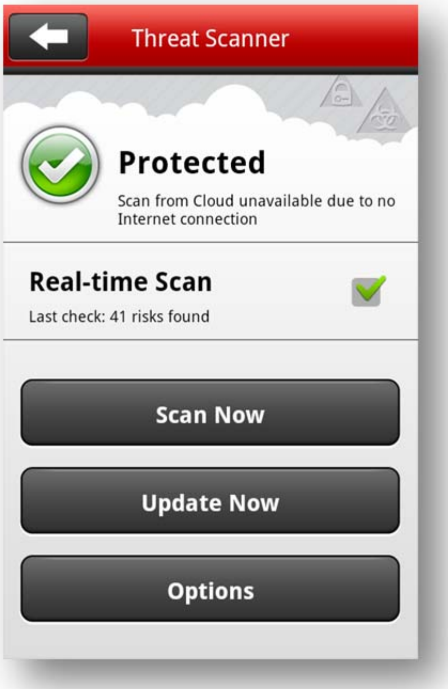
### Installation

We received the installation file from Trend Micro. Installation involved starting the setup file from the file explorer and giving the program appropriate permissions.

### Starting the program

When the program is first started, the user has to create a Trend Micro account (or use an existing one). A short configuration wizard then appears, which makes clear the possibilities in the context menu, and assists with the activation of the device administrator. The start screen then appears, with messages informing the user that the Data Protection, Security and Theft Protection features need to be configured.

### Threat Scanner


Threat Scanner

Protected

Scan from Cloud unavailable due to no Internet connection

Real-time Scan ✓

Last check: 41 risks found

The Threat Scanner checks the device for malware. Additionally, it is possible to scan the phone with a cloud service. The Real-Time Scanner is activated by default, and scans new apps when they are installed. The On-Demand Scan checks all installed apps and data on the phone.

The virus definitions can be updated every day, week or month, and a scan can be set to start automatically after every update.

### Data Protection Scanner

Some malware programs are designed to steal personal data. The Data Protection Scanner warns the user of apps that may attempt to do this. The real-time protection checks all apps as they are installed, and an On-Demand Scan can check the memory card as well.

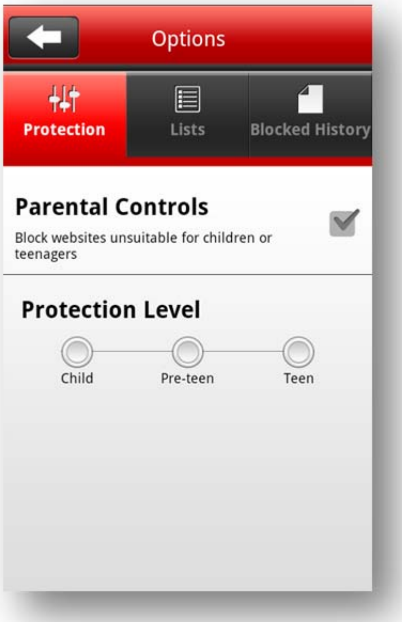
### Security

The Security menu contains the items Safe Surfing, Parental Control, Call Blocking and Text Blocking. Only the Parental Control function is not activated by default.

#### *Safe Surfing*

Safe Surfing protects against fraudulent websites and those pushing malware or other dangers. Three levels of protection are available: low, standard and high. In addition, specific websites can be blacklisted or whitelisted.

## *Parental Control*



Parental Controls ☑
Block websites unsuitable for children or teenagers

Protection Level
○ Child ○ Pre-teen ○ Teen

The Parental Control feature blocks web pages that parents consider unsuitable for their children, such as drugs, weapons, and social networks. There are three levels of protection for three different age groups: child, juvenile and teenager, with appropriate blocking criteria for each. Detailed information is available to users in the help function. Reducing the level of parental control below Teenager is not possible, but individual websites can be blacklisted or whitelisted.

## *Call Blocking*

Call blocking prevents nuisance calls, and can be configured contact by contact. Trend Micro allows for three different configuration options: only blacklisted numbers are blocked; only whitelisted numbers are allowed; only whitelisted and anonymous callers are allowed.

It is also possible to configure the action to be taken in the event of a call from a blacklisted number: the call can be rejected, with our without a message being sent to the caller or the phone can be set not to ring.

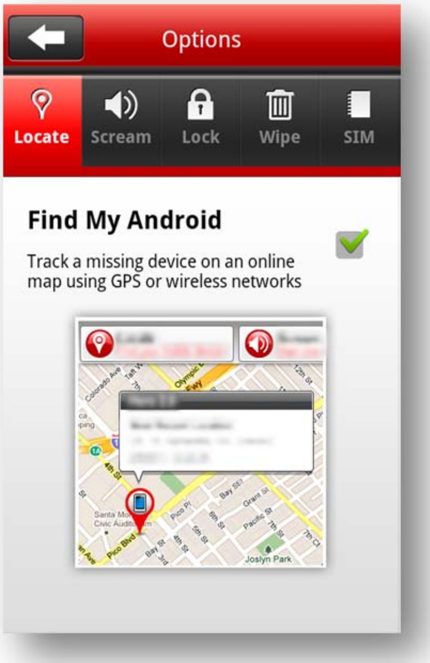
## *Text-message blocking*

Text-message blocking rejects SMS messages from specified numbers. Trend Micro uses the blacklisting/whitelisting principle; either all numbers are allowed, except those on the blacklist or no numbers are allowed, except those on the whitelist. The action to be taken when a blocked message is sent can be configured too: the options are block only, block and delete, or block and send a reply. It is also possible to filter messages using keywords.

## Loss protection

Loss Protection includes all features to be used in the event that the mobile phone is lost or stolen. Administration is via a web interface.

As well as the functions Find My Android and enabling/disabling SIM Card Lock, the Loss Protection area includes descriptions and diagrammatic representations of the anti-theft features. Additionally, the Find function can be activated or deactivated. The Yell, Lock and Wipe features cannot be deactivated. All features are active by default.



Find My Android ☑
Track a missing device on an online map using GPS or wireless networks

### *Find*

The Find function locates the mobile phone and shows its location in Google Maps. The exact address and the time of the location reading are also shown.

Trend Micro mentions "pursuit" in the description of the feature, although it does not have the ability to actually track the phone by showing the route it has been taken on.

### *Scream*

The Scream feature serves to help the owner find the phone if it has been mislaid or stolen. Scream emits a loud noise that stops again after a minute.

### *Lock*

When the Lock function is used, a lock screen is shown on the phone, preventing unauthorised access. The password has to be entered in order to start using the phone again.

### *Wipe*

The Wipe function resets the phone to factory settings, deleting all personal data in the process.

#### Google account

The reset process disabled access to the Google account, making emails, calendar, Google Play etc. inaccessible from the phone.

#### Data recovery

It was possible to recover a majority of the data on the internal storage, but nothing from the removable SD card.

### *SIM Card Lock*

This feature locks the phone if a different SIM card is inserted, to prevent its use by unauthorised persons. The phone can only be used again if the correct password is entered.

### Web Interface

Trend Micro, like many vendors, uses a web interface to administer the theft-protection features.

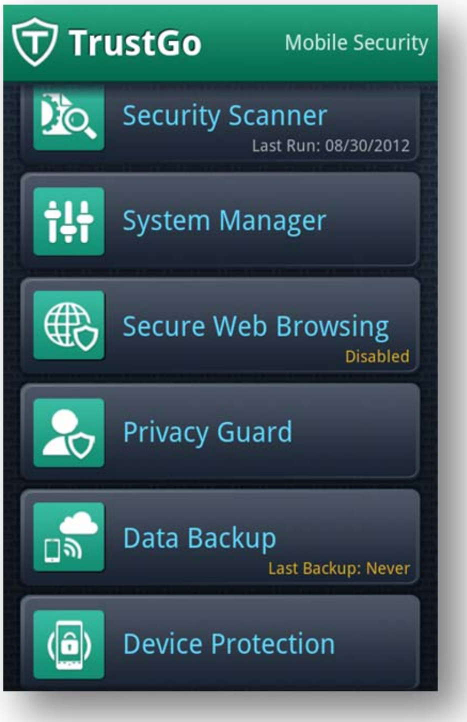
### Conclusion

Trend Micro has produced a well-designed security product with a consistent user interface.

We particularly liked the help function for the individual components, as well as the web interface, which allows multiple devices to be administered from the same console.

## TrustGo Antivirus & Mobile Security

Antivirus & Mobile Security by TrustGo enables the user to administer the program using a clear and simple web interface. As well as providing antivirus and theft protection, the suite also includes a backup solution.



### Installation

We downloaded and installed TrustGo Mobile Security from Google Play. Setup was a very short process and only required the acceptance of a licence agreement and the creation of a TrustGo user account.

### Starting the program

On starting the program for the first time, the user is taken straight to the home page of the program without any questions or messages. As no additional help is provided, it is up to the user to find their own way around the software's features.

No scans or backups take place automatically after starting the programm. However, reminder messages in the form of small yellow lettering on each function's button are intended to remind the user to configure these items.

### Finding Trustworthy Apps

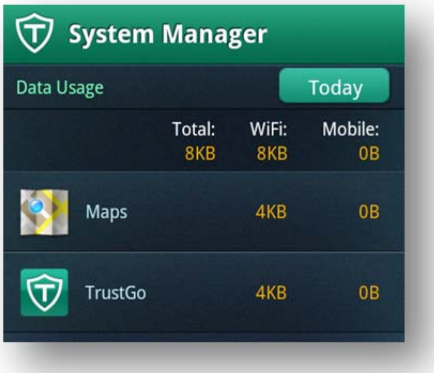
Finding Trustworthy Apps is a search for apps on markets examined and classified by TrustGo.

### Immediate Virus Scan

This feature starts a manual virus scan. This can be configured to scan only apps or the memory card as well. Scans can be configured to run on a weekly or monthly basis.

### System Manager

System Manager provides an overview of the data volume used, battery status and data storage used. Selecting one of the three functions produces a detailed display; in the case of data usage, this differentiated between data sent by Wi-Fi and data sent via the mobile phone network, which we found very useful. The amount of data that can be transferred every month (in accordance with the user's mobile phone plan) can be entered; the software calculates when 90% of this has been used and shows a notification.



| | Total: | WiFi: | Mobile: |
|---|---|---|---|
| | 8KB | 8KB | 0B |
| Maps | | 4KB | 0B |
| TrustGo | | 4KB | 0B |

### Safe Web Browsing

The Safe Web Browsing feature protects the user from websites considered to be harmful. There are no settings for this feature, except to deactivate it completely. TrustGo is currently the only product which supports the Dolphin browser with its Safe Web Browsing.

### Privacy Protection

Privacy Protection groups apps according to their access rights to saved contacts, text messages, personal information etc. It is possible to select individual apps from the groups and uninstall them directly. We liked the fact that TrustGo's certification for the apps is shown.

## Data backup

The Data Backup menu allows the user to select from contacts, text messages and call history to back up in the cloud. Unfortunately, it is not possible to back up any other data, such as photos.

The recovery of data is also controlled from this menu. It should be noted that the backup process creates a snapshot of the current data set, which can be restored if necessary; any data created or modified between the last backup and the restore will be lost.

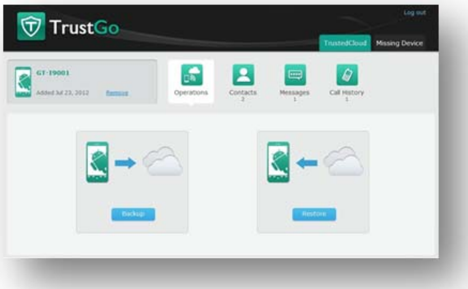
As with the virus scanner, this function can be scheduled for automatic execution.

## Device Protection

Device Protection contains TrustGo's theft protection features. These enable the user to locate the phone and protect their privacy in the event of loss or theft. Administration is carried out via web console. Apart from total deactivation, there are no configurable settings for the theft protection features.

Other features are available in the Device Protection menu. For example, Self Protection, which prevents accidental removal of the TrustGo suite. Activation of this feature is necessary to reset the device to factory settings. TrustGo has to be set as the device administrator here. This section also allows a message to be created which will be shown on the phone in the event that the remote lock function is used.

## Web Interface



The web interface [9] is very intuitive and also aesthetically well designed. It provides an overview of the data saved by the backup feature, and enables both backup and restore actions to be started.

The theft protection functions are also accessible from the web interface. Additionally, there is also a mobile version of the web interface available.

### *Lock*

The web interface allows the device to be locked and unlocked. A message to be displayed on the screen if the lock feature is used can be defined here, along with the user's name and contact details.

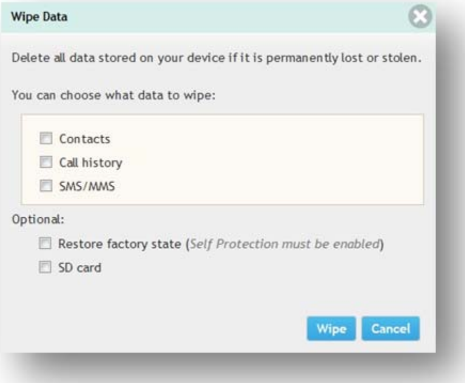
The mobile phone can be unlocked either by using a self-choosen password or by using a 16-digit unalterable code.

### *Alarm*

This function causes the device to emit a penetrating alarm sound, and simultaneously locks it. The phone can then only be unlocked by entering the correct code; this can also be done from the web console.

[9] http://www.trustgo.com

### *Wipe*


Wipe Data

Delete all data stored on your device if it is permanently lost or stolen.

You can choose what data to wipe:

□ Contacts
□ Call history
□ SMS/MMS

Optional:

□ Restore factory state (*Self Protection must be enabled*)
□ SD card

The Wipe function can be used to delete personal data from the phone. The user is given options as to which data to delete. To return the device to factory settings, the Self Protection feature must already have been activated.

#### Google account

Even if the device is returned to factory settings, the credentials for the Google account are not deleted. If the contacts are then synchronised, the effect will be that all contacts are deleted from the Google account.

#### Data recovery

After using the Wipe function, we were able to recover the majority of the data using a recovery tool.

### Conclusion

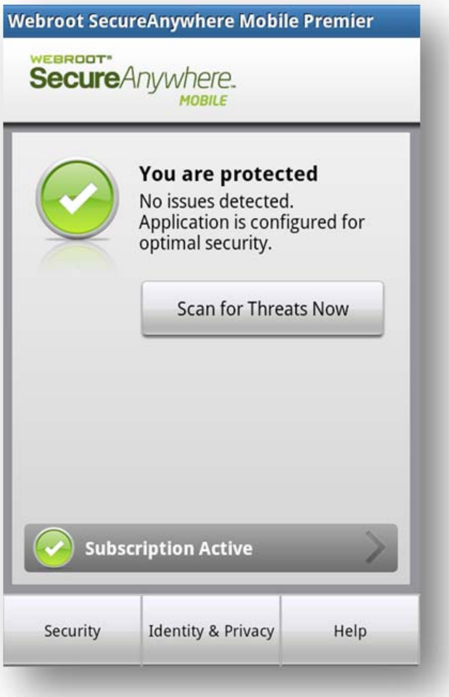
TrustGo Antivirus & Mobile Security offers comprehensive features. We particularly liked the well-structured System Manager feature, which displays battery usage and the volume of data transferred.

In order to prevent a complete loss of contacts data from a Google account, we feel that TrustGo should ensure that the Wipe function also deletes the access credentials for the Google account.

We would also like to see some sort of help function to explain each of the features and how to use it; this is currently not included.

## Webroot SecureAnywhere Mobile Premier

Webroot SecureAnywhere Mobile Premier is a comprehensive security product that gives the impression of being well thought-out. This includes the consistent web interface, which allows the administration of multiple devices from one account.


Webroot SecureAnywhere Mobile Premier
WEBROOT SecureAnywhere MOBILE
You are protected
No issues detected.
Application is configured for optimal security.
Scan for Threats Now
Subscription Active
Security
Identity & Privacy
Help

### Installation

Webroot SecureAnywhere Mobile is currently available in version 2.9 from the Google Play Store. Downloading and installing the application was a very straightforward process.

### Starting the program

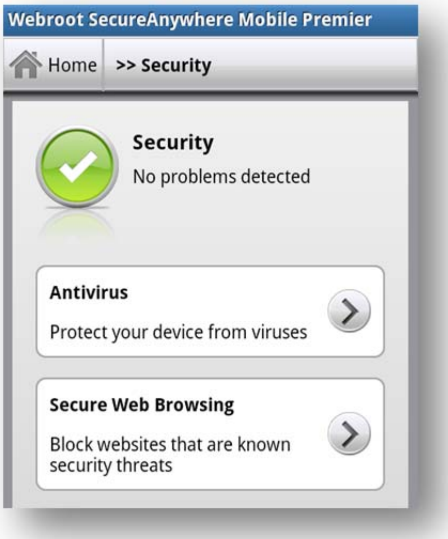
When starting the program for the first time, the user has to accept the licence agreement. A welcome message with information and notices for the user then appears.

If the user does not already have a Webroot account, this has to be created as the next step in order to access the web interface. This involves entering an email address, telephone number and password. The URL of the web interface is then displayed.

The Premium version of Webroot SecureAnywhere Mobile can be obtained directly from Google Play, or the free version can be upgraded by registering it.

After a successful upgrade, the user is informed of any problems and their possible solutions. In our test, we were informed of the activated USB-debugging, as Webroot classifies this as “insecure” and points the user to password protection for deinstallation and administrator settings.

### Security


Webroot SecureAnywhere Mobile Premier
Home
>> Security
Security
No problems detected
Antivirus
Protect your device from viruses
Secure Web Browsing
Block websites that are known security threats

The Security settings allow the user to configure the antivirus component of the suite, and activate or deactivate the secure web browsing feature.

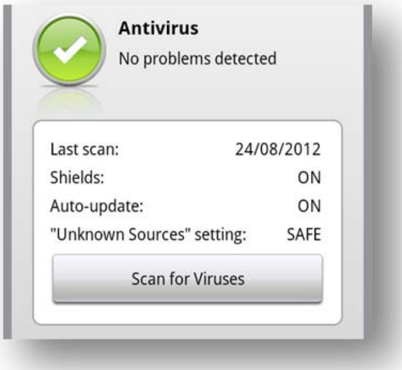
### *Anti-Virus*

This allows the user to check the mobile phone for malware and configure the protection component. Scans and updates can be set to run automatically according to a timetable, with the options Never, Hourly, Daily or Weekly available.

The protection features include Installation Protection, which checks new apps on installation; File System Protection, which scans new or changed files; Execution Protection, which scans every app each time it is run. Additionally, Protection from Unknown

Sources and USB Debugging Protection can be activated or deactivated.

We were particularly pleased to see that there is an overview of all the antivirus components and their status:


Antivirus
No problems detected

Last scan: 24/08/2012
Shields: ON
Auto-update: ON
"Unknown Sources" setting: SAFE

## Identity and Privacy

This feature enables the identity and privacy of the user to be protected in the event that the device is lost or stolen. Calls and text messages from specified numbers can also be blocked.

### *Device Loss Protection*

This component is activated by default. With the help of the web interface or text messages, it allows the user to locate/lock/wipe the phone remotely, or to send out a warning signal.

Webroot also has a protection mechanism to guard against change of SIM card. SIM Card Lock locks the telephone if the card is replaced; it can then only be unlocked with the correct password.

### *Call and Text Blocking*

The Call and Text Blocking feature is a useful addition to the suite's features. It enables the user to add contacts and phone numbers to a blacklist; any attempts to contact the user from the relevant numbers/addresses are then blocked. This helps protects against e.g. stalking.

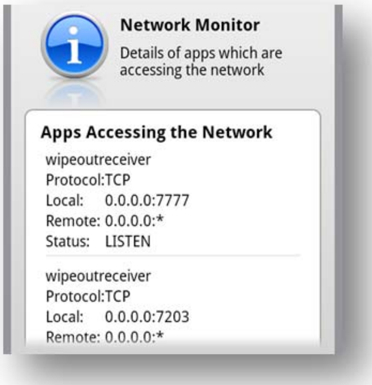
Additionally, the suite blocks by default any text messages containing links to known phishing sites.

Finally, we should mention the possibility of blocking unknown caller IDs. When this feature is activated, calls and texts from unknown numbers will not be accepted.

The description of this function is unclear. It states that calls and texts from unknown caller-IDs will be blocked. Whether this means withheld numbers, or simply those that are not in the user's address book, we don't know.

### *App Checker*

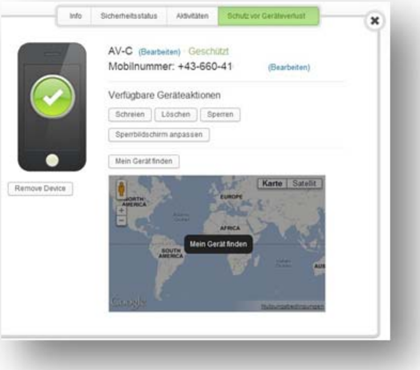
The App Checker analyses any apps that could be a security risk, and lists all apps according to their battery usage. There is also a network monitor, showing the network connections of installed apps. This feature requires technical knowledge to be of any value, and so is probably not very helpful to the standard user.


Network Monitor
Details of apps which are accessing the network

Apps Accessing the Network
wipeoutreceiver
Protocol:TCP
Local: 0.0.0.0:7777
Remote: 0.0.0.0:*
Status: LISTEN

wipeoutreceiver
Protocol:TCP
Local: 0.0.0.0:7203
Remote: 0.0.0.0:*

## Web Interface



AV-C Geschützt
Mobilnummer: +43-660-41

Verfügbare Geräteaktionen

The web interface is very modern and gives a clear overview. As well as information about the software version, it provides security status and activity reports, and access to the theft-protection features.

### *Locking*

This function allows the phone to be locked remotely, preventing unauthorised access in the event of loss or theft. A message can also be displayed on the screen that allows an honest finder to return the phone to its owner. The phone is supposed to remain locked until the right password is entered to unlock it.

In our test on a Samsung Galaxy S plus device, we were able to get around the lock by clicking Emergency Call and then pressing the Home button. On a Samsung Galaxy S3 device, it was not possible to make emergency calls while the phone is locked. Webroot informed us that they are going to improve the lock screen functionality in the 3.0 release so that the lock screen cannot be bypassed in any manner. The fix for Galaxy S3 has now been already released.

The device can be locked through the web interface or by sending a text message with the content “lock [password]”.

### *Scream*

The Scream function causes the phone to emit a penetrating alarm sound, and simultaneously locks the device.
The function can be activated through the web interface or by sending a text with the content “scream [password]”.

### *Wipe*

The Wipe function deletes all personal information on the phone. This can be initiated from the web interface, or by texting “wipe [password]” to the phone. As a result, the device is reset to factory settings, resulting in the deletion of all personal data.

#### Google Account

The return to factory settings removes the login details for the Google account. This makes it impossible to access mails, contacts, Google Play etc. from the phone.

#### Data recovery

With the help of a recovery tool, it was possible to restore the majority of the deleted data.

### *Find Device*

This function allows the phone to be located remotely. Its position is shown on a map in the web interface; the device is simultaneously locked. Find Device can be activated by texting “locate [password]” to the phone.

### Conclusion

SecureAnywhere Mobile Premier is a powerful, well-designed security product, and Webroot have paid attention to detail. Theft protection functions can be activated using the web interface or by text message.

The web interface, which allows the administration of multiple devices from one account, impressed us with its consistent design and intuitive user interface.

Our one complaint is the ability to circumvent the screen lock on the Samsung Galaxy S plus device by use of a trick, and we urge Webroot to rectify this as soon as possible.

## Conclusion

Smartphones do get stolen, but far more get lost. Every day, people lose smartphones worth 7 Million US Dollars[10] (5.3 Million Euro at the time of writing). The loss of the device is not just very annoying to the owners, but creates a risk that they often underestimate. When unauthorised persons get hold of a smartphone or tablet, they often have access to personal data such as the address book or personal photos. Installed shopping apps may allow them to make purchases online, at the expense of the owner.

Therefore it is very important to bring home to users that security software on their smartphones is just as essential as security software on their home PCs.

In our test last year, many manufacturers were unable to cleanly delete Google-account login credentials. Almost all of them have now rectified this. However, some of the security software providers still do not erase the SD card effectively in a remote wipe procedure. Data stored on it can in many cases still be recovered with a free tool, as happened last year.

All the products we tested served their purpose, but it is difficult to say which product is best for which user. Prospective buyers should consider which protection features are most important to them, and then look for a product which does well in this category. Almost all manufacturers provide a free test version of their product. In any event, we would recommend a product that includes at least virus and web protection, and a remote lock.

[10] http://www.chipchick.com/2012/04/lost-phones.html

| Feature List Mobile Security | FREE | COMMERCIAL | FREE | COMMERCIAL | COMMERCIAL | FREE | COMMERCIAL | FREE | COMMERCIAL | COMMERCIAL | COMMERCIAL | FREE | FREE | COMMERCIAL | FREE | FREE | COMMERCIAL | FREE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Product name: | avast! Free Mobile Security 2.0 | Bitdefender Mobile Security 2.0 | Bitdefender Mobile Security FREE 2.0 | ESET Mobile Security 1.1 | F-Secure Mobile Security | F-Secure Anti-Theft | IKARUS mobile.security | IKARUS mobile.security LITE | Kaspersky Mobile Security 9.4 | Lookout Premium | McAfee Mobile Security | Qihoo 360 Smartphone Guard 3.1 | Sophos Mobile Security 1.0 | Trend Micro Mobile Security Personal Edition 2.5 | Trend Micro Mobile Security Personal Edition 2.5 FREE | TrustGo Antivirus & Mobile Security 1.2.0 | Webroot SecureAnywhere Mobile Premier 2.9 | Webroot SecureAnywhere Mobile 2.9 |
| Supported OS versions: | Android 2.1 and up | Android 2.2 and up | | Android 2.0 and up | Android 2.2 and up | | Android 2.2 and up | | Android 2.2 and up | Android 2.1 and up | Android 2.1 and up | Android 2.1 and up | Android 2.2 and up | Android 2.2 and up | | Android 2.2 and up | Android 2.1 and up | |
| Supported Program languages: | English, Italian, Polish, Czech, Japanese, Portuguese, Spanish, French, Hungarian, Croatian, Russian, Dutch, German, Chinese | English, Portuguese, Spanish, Italian, German, French, Romanian | | English, Polish, Danish, Finnish, Norwegian, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Swedish, Chinese, Italian, Korean, Spanish, Latin, Czech, Hebrew, Slovak | English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish | | German, English, Italian, Chinese | | English, Russian, French, German, Italian, Spanish, Portuguese, Polish, Japanese, Chinese, Korean, Dutch, Finnish, Norwegian, Sweden, Danish | English, Russian, Korean, Chinese,German, French, Japanese, Spanish, Portuguese, Polish | English, Chinese, German, French, Italian, Japanese, Dutch, Spanish, Portuguese, Indonesian, Korean, Swedish, Russian, Norwegian, Danish, Finnish, Greek | Chinese | English, German, French, Japanese | English, Japanese, Chinese, French, Dutch, Italian, Spanish, Korean, Russian, Portuguese, Turkish | | English, German, Japanese, Korean, Russian, Spanish | English, Japanese, Spanish, Portuguese, French, German | |
| Anti Spam | | | | | | | | | | | | | | | | | | |
| Whitelist/Blacklist SMS | ● | | | ● | ● | | ● | | ● | | ● | ● | | ● | | | ● | ● |
| Whitelist/Blacklist calls/MMS | ● | | | ● | ● | | | | ● | | ● | ● | | ● | | | ● | ● |
| Block known SMS/MMS spam | ● | | | | | | | | | | ● | ● | | ● | | | ● | ● |
| General blocking of known/unknown contacts and hidden numbers | | | | ● | | | | | | | | ● | | ● | | | ● | ● |
| Block Phone calls, email, SMS/MMS, Web-Browsing, apps between specified hours | ● | | | | | | | | | | | | | | | | | |
| Parental Control | | | | | | | | | | | | | | | | | | |
| Locate phone by SMS | ● | ● | | ● | ● | ● | ● | | ● | | | Only Mainland China | ● | | | | ● | ● |
| Lock apps | | | | | ● | | | | | | | ● | | | | | | |
| Anti-Bullying /Anti-Sexting-SMS/MMS/Emails/IM-Chats | | | | | ● | | | | | | ● | | | | | | | |
| Make the device call you back so you can hear what's happening around it | ● | ● | | | | | | | | | | | | | | | | |
| Log all visited URLs | | | | | | | | | | | | | | ● | | | | |
| Remote Features | | | | | | | | | | | | | | | | | | |
| Remote GPS localization | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● | Only Mainland China | ● | ● | | ● | ● | ● |
| Remote wipe | ● | ● | | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | ● | ● | |
| Remote lock | | ● | | ● | ● | ● | | | ● | ● | | ● | ● | ● | | ● | ● | ● |
| Remote alarm | | ● | | | ● | ● | ● | | | ● | | | ● | ● | | ● | ● | ● |
| Remote tower id / wifi location | | ● | ● | ● | | | | | ● | | | | | ● | | ● | ● | ● |
| Remote configuration | ● | | | | ● | ● | | | | | ● | ● | | | | ● | | |
| Remote unlock | | | | ● | ● | ● | | | | | | ● | | | | ● | | |
| Authentication | | | | | | | | | | | | | | | | | | |
| Lock  Screen with Password protection | | ● | | ● | ● | ● | ● | ● | ● | | ● | | | ● | | ● | ● | ● |
| Password policy: Strength, length, etc. | ● | | | | ● | ● | ● | | ● | | | ● | | | | ● | ● | ● |
| Access control | ● | | | | ● | ● | ● | | ● | | | ● | | | | ● | | |
| Maximum number of failed attempts | | | | | ● | ● | | | ● | | | | | | | ● | | |
| Grace period | | | | | ● | ● | | | | | | | | | | ● | | |
| Anti-Malware | | | | | | | | | | | | | | | | | | |
| Real Time App protection | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| On Demand Scan | ● | ● | ● | ● | ● | | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● |
| Cloud Scanning (requires cloud connection) | | ● | ● | | ● | | | | ● | ● | | ● | ● | ● | ● | ● | | |
| Prevent access to harmful web sites | ● | ● | | | ● | | | | ● | ● | ● | | | ● | | ● | ● | ● |
| Scheduled Scan | ● | | | | ● | | ● | ● | ● | | ● | | ● | | | ● | ● | ● |
| Application Audit / Security info about installed apps | | ● | ● | ● | | | | | | ● | | ● | ● | | | ● | ● | |
| Different Update profiles | | | | | ● | | ● | ● | | | | ● | ● | | | | ● | ● |
| Own roaming update profile | ● | | | | ● | | | | | ● | | ● | ● | | | | | |
| SMS/MMS Scanner | ● | | | | ● | | | | | | ● | ● | | | | | ● | ● |
| Quarantine | | | | ● | | | | | | | | ● | | | | | ● | ● |
| Black-/whitelist for web browsing | | | | | | | | | | | | | | ● | | ● | ● | ● |
| Network protection | ● | | | | | | | | ● | | | ● | | | | ● | | |
| Block attachments/applications/file extensions | | | | | | | | | ● | | | | | | | | ● | ● |
| Anti-Theft | | | | | | | | | | | | | | | | | | |
| Possibility to make emergency calls while locked | | ● | ● | ● | ● | ● | | | ● | | ● | ● | | ● | | ● | ● | ● |
| Web Interface for remotely managing the phone in case it gets stolen | ● | ● | ● | | ● | ● | | | | ● | | | | ● | | ● | ● | ● |
| Report thief's phone number by SMS | ● | ● | | ● | ● | ● | | | ● | | ● | ● | ● | | | | | |
| Lock Contacts | | | | | ● | ● | | | ● | | ● | ● | | | | | ● | ● |
| Lock Images/Files, SMS/MMS | | | | | ● | ● | | | ● | | ● | ● | | | | | ● | ● |
| Possibility to receive calls while locked | ● | ● | ● | | ● | ● | | | | | | ● | | | | | | |
| Report thief's location at SIM change | ● | ● | | ● | | | | | ● | | ● | ● | | | | | | |
| Lock SIM | | | | | | | | | | | ● | | | ● | | | ● | |
| Backup | | | | | | | | | | | | | | | | | | |
| Backup of SMS/MMS, contatcs and user data (online / memory card) | | | | | ● | | | | | ● | ● | ● | | | | ● | | |
| Backup Call History | | | | | | | | | | ● | | | | | | ● | | |
| Scheduled data backup | | | | | | | | | | ● | | | | | | ● | | |
| Support | | | | | | | | | | | | | | | | | | |
| Phone Support, Email Support | ● | ● | ● | ● | ● | ● | ● | ● | ● | Only E-Mail | ● | ● | ● | ● | ● | ● | ● | ● |
| User Forum, Online Help | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Online Help (special URL designed for browsing with the phone) | ● | | | ● | ● | ● | | | ● | ● | ● | ● | ● | ● | ● | | ● | ● |
| User manual | ● | ● | ● | ● | ● | ● | | | ● | ● | ● | ● | ● | | | | ● | ● |
| Online Chat | | ● | ● | ● | ● | ● | | | | | ● | ● | | ● | ● | ● | ● | ● |
| Supported languages (of support) | English, German, French, Spanish, Portugese, Russian, Japanese, Turkish, Ukranian, Czech, Slovak, Italian, Polish | English, French, German, Romanian | | All | English, Finnish, French, Dutch, Danish, German, Chinese, Italian, Norwegian, Polish, Swedish | | English, German | | English, Russian, French, German | English, Spanish, German, French, Polish, Portuguese, Russian, Chinese, Japanese, Korean | English, Chinese, Japan, Korean, German, Dutch, Danish, French, Finnish, Italian, Norsk, Polish, Portuguese, Russian, Swedish, Czech, Turkish | Chinese | English | English, German, French, Italian, Dutch, Danish, Norwegese, Swedish, Spanish, Russian, Japanese, Taiwanese | | English, Russian, Chinese | English, Japanese, Spanish (email any) | |
| Additional features | | | | | | | | | | | | | | | | | | |
| Statistics | ● | | | ● | ● | ● | ● | ● | ● | ● | ● | ● | | | | ● | ● | ● |
| Account (not device) based licensing - same license for multiple devices if same owner | ● | ● | ● | ● | ● | ● | | | | | | ● | ● | ● | ● | ● | ● | ● |
| PW protection of uninstallation | | ● | | ● | ● | ● | ● | | ● | | ● | | | ● | ● | ● | ● | |
| SIM Watch (changing the SIM) | ● | ● | | ● | ● | ● | | | ● | | ● | ● | ● | ● | | | ● | |
| No SIM activation | ● | ● | ● | ● | ● | ● | | | ● | ● | | ● | | | | | ● | ● |
| Central Management | ● | | | | ● | ● | | | ● | ● | ● | ● | | | | ● | ● | ● |
| Password protection for settings | | ● | ● | ● | ● | ● | | | ● | | | | | ● | | | ● | ● |
| Battery Monitor, Task Killer | | | | ● | | | | | | | | ● | | | | ● | ● | |
| Several trusted SIM cards | | | | ● | ● | ● | | | | | | | | | | | | |
| Offline activation | | ● | ● | | | | | | | | | ● | | | | | | |
| Data network usage monitor | ● | | | | | | | | | | | | | | | ● | | |
| Storage Monitor | | | | ● | | | | | | | | | | | | | | |
| File Shredder | | | | | | | | | ● | | | | | | | | | |
| Price (may vary) | | | | | | | | | | | | | | | | | | |
| Price 1 phone / 1 year (USD/EUR) | FREE | 10 USD / 7 Euro | FREE | 10 USD / 7 Euro | 25 USD / 20 Euro | FREE | 20 USD / 15 Euro | FREE | 30 USD / 25 Euro | 30 USD / 25 Euro | 30 USD / 30 Euro | FREE | FREE | 30 USD / 25 Euro | FREE | FREE | 20 USD / 15 Euro | FREE |
| Price 3 phones / 2 years (USD/EUR) | FREE | 20 USD / 15 Euro | FREE | 20 USD / 15 Euro | 150 USD / 120 Euro | FREE | 60 Euro / 45 Euro | FREE | 180 USD / 150 Euro | 180 USD / 150 Euro | 180 USD / 180 Euro | FREE | FREE | 180 USD / 150 Euro | FREE | FREE | 40 USD / 30 Euro | FREE |

## Copyright and Disclaimer

AV-Comparatives e.V. 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 e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (September 2012)

Portions of this report are modifications based on work created and shared by the Android Open Source Project and used according to terms described in the Creative Commons 2.5 Attribution License. Pictures: © iStockphoto.com, © AV-Comparatives

X TEST

## x.test introduction

x.test is the leading supplier for electronic test and measurement for Agilent Technologies, Flir and Haefely in Austria.

We offer the broad product portfolio from simple handheld DMMs over ESD measurement systems, from thermografic solutions to oscilloscopes, up to spectrum- and network analyzer for RF and microwave measurement tasks.

Please, fell free to contact us for your T&M task:

**x.test GmbH**
**Amalienstraße 48**
**1130 Vienna**
**Austria**

phone: +43 (1) 8778 171 - 0
e-mail: info@xtest.at
web: www.xtest.at

## FLIR

Since April 1st, 2012 x.test is responsible for cooled and not-cooled thermografic cameras for research and development from Flir systems in Austria.

**T450SC**

- IR resolution: 320x240 pixel
- Therm. Sensitivity/NETD: 40mK
- picture framerate: 60Hz

## Agilent Technologies

**X-series Signal Analyzer**
**CXA, EXA, MXA, PXA, MXE –** from Low Cost spektrum analysis up to EMC full-compliance test!

www.agilent.com/find/xseries

**DC Power Analyzer** – flexible and DC-power supply

4 slots
600W, > 20 modules

www.agilent.com/find/N6705B

## HAEFELY TECHNOLOGY EMC

Since October 1st, 2011 x.test is the official sales represantent for Haefely EMC in Austria and helps you with your ESD/Surge/Burst/EFT-measurment task!

ONYX

**16kV or 30kV ESD Simulator**
www.haefely-onyx.com

Ergonomic ESD-simulator without bases-station for 16kV or 30kV testing. Touchscreen, LED-tip, replaceable RC-Module, and more.

axos5

**Compact immunity test system**
Multifunctiongenerator for following conducted transients: Burst/EFT, Surge Combination Wave (1.2/50us…8/20us) and AC/DC Dips & Interruptions up to a maximum voltage of 5.0kV

www.haefely.com/axos5