Product Review

Mobile Security Review

Language: English
August 2011
Last revision: 28th September 2011
www.av-comparatives.org

Contents

Introduction

Smartphones are becoming ever more popular. As mini-multifunction devices, they are slowly but surely replacing "phone only" devices. Above all, it is the messaging and Internet capabilities that make these mini-computers so desirable. These features bring risks, however.

It is precisely the connectivity features that make smartphones interesting for criminals who attempt to infect phones with malware, or steal private data, either directly from the phone or through phishing attacks.

The use of a desktop or laptop PC without virus protection has become unthinkable. Yet smartphones seem to go unnoticed when it comes to protection, despite the fact that many are used to store private photos and data, or even company data.

Smartphones are small and expensive, making them an attractive target for thieves. It must be made more difficult for thieves to gain access to private data, in order to reduce the appeal of stealing smartphones. Without security precautions for smartphones, life is easy for criminals. Thieves steal smartphones, change the SIM card (making it unreachable for the owner), or make calls at the owner's expense, possibly for further criminal activity. To prevent things like this happening, today's security suites for smartphones have a range of features.

Theft Protection

Theft protection for smartphones is a very useful feature. In the event that his/her smartphone is lost or stolen, the owner can locate it, using the phone's built-in GPS function; lock it, to prevent anyone else using it; or wipe it, to prevent private data being stolen. To locate a lost or stolen phone, the owner can use any other mobile phone to send a text message (SMS) to his/her phone; a text message will be sent back with the GPS co-ordinates of the phone's current location. In some cases, a web interface can be used to do the same thing.

The location function is very useful, although it should be noted that it can be misused to determine the location of people. It is possible to install a security product on somebody's phone in order to track their whereabouts; an apparently kind gift of a smartphone with such software pre-installed could also be used for the same purpose.

This year, a new trend has appeared, in that many manufacturers are using web-based controls for theft protection features, although some have stuck with the text message approach.

Virus protection

The malware protection element of smartphone security suites searches the phone for malicious programs, and deletes or quarantines any it finds. For this feature to work efficiently, virus updates have to be kept up to date. Users should be aware, however, that the download of virus definitions may cause high data roaming charges when travelling abroad.

This year, we have tested security products for Google's Android operating system, on account of its growing market share (41.8%). Support for other operating systems can be seen in the features list.

Smartphones are not the only communication devices for which security products must be considered. In future, there may be security risks for all home entertainment devices (such as Internet-ready TVs), which will need their own security solutions.

This report contains details of the products made by leading security software providers who agreed to have their software tested by us.

The test was carried out in August 2011 using an LG P500 smartphone running Android 2.2, German version. Where the security products were downloaded from the Android Market, we accepted the default version; with two of the products, this meant that the German version of the program was installed.

Malware detection

The review concentrates on the features and ease of use of the products, rather than malware detection.

However, we didn't want to ignore malware protection completely. Therefore we tested the products with a very small sample of malicious programs, in order to check their basic functionality.

We feel that Android malware on the WildList, i.e. current, common malware, should be recognised. Malware from this list is frequently used to certify AV products.

The Extended WildList [1] from July 2011 contains Android malware samples found "in the wild", and these were used for our test.

BlackBelt, BullGuard, ESET, F-Secure, McAfee, Vipre and Webroot recognised all of the samples. Kaspersky also recognised them once we had carried out a manual update after installation. Trend Micro's product, however, failed to recognise malware from the BaseBridge family; very surprisingly, Trend's product for Windows Desktop PCs did recognise it.

We informed the manufacturers of the results of the test before publication of this report, allowing them to update/improve their products. All the samples are now recognised by all the tested programs.

Significant flaws

None of the products deleted all of the data irretrievably in the remote wipe test. In all cases it was possible to recover photos, music, documents and so on from the external storage card, even using a free program.
More worrying still is the handling of the Google Mail account we had set up on the phone. In most cases, only the data was deleted, not the account, or even its password. Kaspersky was a praiseworthy exception.
Unless the user remembers to change the password for the Google account before running the remote wipe process, a thief will still be able to access the owner's emails. In the event that the account is synchronised between phone and server (which may happen automatically), the contacts data will be globally deleted from the Google account, not just from the phone.

We would strongly recommend that the interface of Android security products should remind users to change the password to their Google accounts before using the remote wipe feature.

Some manufacturer's products simply reset the phone to factory settings when the remote wipe command is issued. This solves the problem of the Google account, but means that the security product itself is removed from the phone, and so can no longer be used to locate the phone or fulfill any of its other functions.

[1] http://www.wildlist.org/WildList/201107_ext.txt

Summary of results

The perfect mobile security product for Android phones has yet to be made. As with other security products, such as those for Windows, the best course of action must be to look at our report and find a few good candidates; trial versions of these can then be installed and tested before purchasing. There is a very high rate of development of Android security programs, so newer and better releases with improvements and new features frequently appear.

Anyone who wants the choice of SMS and web interface for administration should consider Webroot Mobile Security 2.0.

Kaspersky Mobile Security 9 has a very good SMS and call filter, while BullGuard Mobile Security 10 impresses with its well-designed web interface.

Trend Micro Mobile Security 2.0 is also available as a free program for the iPhone. Vipre Mobile Security 1.0 is also free; we tested the beta version, as the RTM version had not been released at the time of the test. Vipre allows all the phones in a family to be put into one administration account.

McAfee helps battery life by only running its backup feature when the phone is on charge. F-Secure Mobile Security 7 allows the phone to be used for emergency calls even when locked; this is a legal requirement in some countries.

BlackBelt Security 2.2 is very simple to use, and activates the Device Lock and SIM Protection components by default.

We found ESET Mobile Security 1.0 to be one of the best-engineered products, and best incorporated into company network administration.

Products Tested

- BlackBelt Security 2.2
- BullGuard Mobile Security 10.0
- ESET Mobile Security 1.0
- F-Secure Mobile Security 7.0
- Kaspersky Mobile Security 9
- McAfee Mobile Security 1.0
- Trend Micro Mobile Security 2.0
- VIPRE Mobile Security 1.0
- Webroot Mobile Security 2.0

BlackBelt Security

BlackBelt Security extends the company's range of mobile security solutions. It combines the standalone products BlackBelt AntiSpam, BlackBelt AntiTheft and BlackBelt AntiVirus in a single security suite.

Installation

Like all of BlackBelt's products, BlackBelt Security can easily be downloaded from the Android Market, and installed automatically.

Starting the Program

When first starting BlackBelt Security, a licence agreement has to be accepted, and a password of between 3 and 16 characters must be entered. Unfortunately there is no complexity check of the password, and "123" was accepted. An update was then carried out; we would have liked to be asked about this, in order to avoid potentially high roaming charges.

The status display, which was initially set to yellow, was a little irritating. When we looked at the detailed view, all individual components were set to green, but the overall status was still yellow. An explanation of this state would be helpful, e.g. setting the status of the AntiTheft component to yellow. The overall status was only set to green after we had entered a telephone number for alerts in Antitheft.

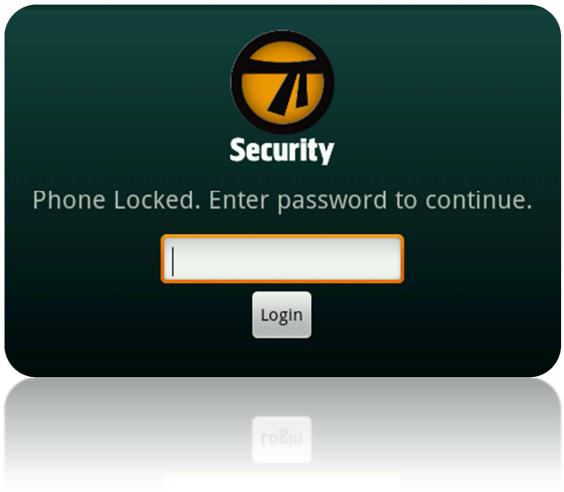
AntiTheft

SIM Protection

BlackBelt AntiTheft is a theft-protection mechanism. The SIM Protection component informs the owner in the event that the SIM card is changed. The owner will also be informed of the telephone number of the new card. The owner can define up to three telephone numbers for messages informing him/her that the SIM card had been changed.

Device Lock

DeviceLock allows the owner to lock the mobile phone remotely. This is done by sending a text message (SMS) with the following content to the device: "!AT [*password]* devicelock", whereby [*password]* is the password defined during installation. Once this has been done, the phone can only be used by entering the password.



It was possible to call the mobile phone once it had been locked, but the finder/thief would have only a fraction of a second to answer, as the password prompt reappears almost immediately. This may make recovering the phone more difficult, however. If the phone has been lost, and found by an honest person, it would be possible to arrange its return by calling the finder, but only if he or she is able to answer the call.

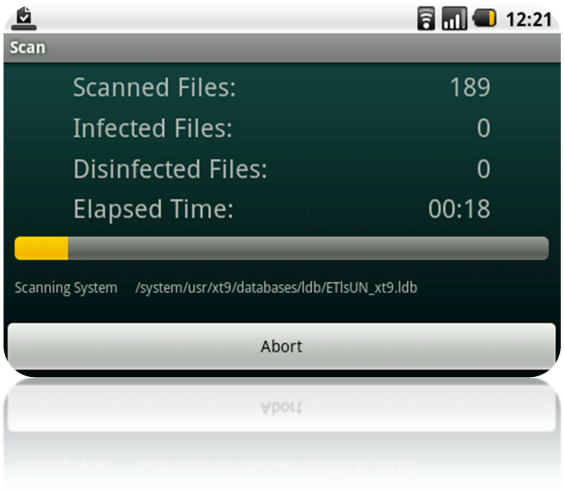
We were pleased to note that BlackBelt activates the SIM Protection and DeviceLock components of AntiTheft by default.

The SIM Protection is only any use, however, if at least one telephone number has been entered. If the owner should forget to do this, he/she will not be informed if the SIM card is changed. This could be avoided if BlackBelt were to run a wizard when the program starts for the very first time, which asked for a phone number to be entered.

We were disappointed to see that when the telephone was locked, it was not possible to make emergency calls.

AntiVirus

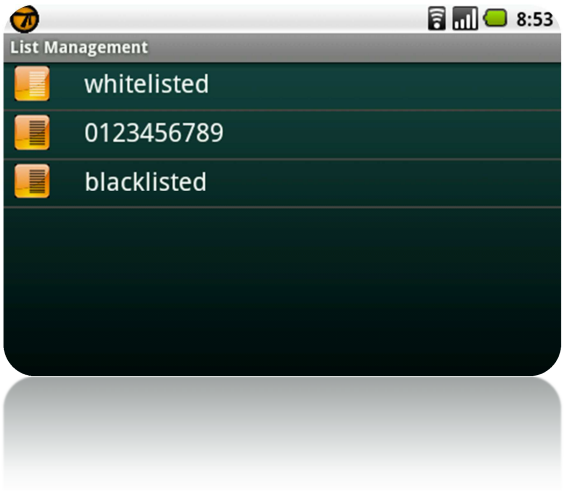
This component scans the mobile phone for malware, and attempts to remove any that is found. An update can be easily initiated.



AntiSpam

BlackBelt's AntiSpam service uses the principles of blacklisting and whitelisting, and applies only to text messaging (SMS). Phone numbers and keywords can be entered into the respective lists, but importing from the address book was unfortunately not possible.

It was also possible to enter a phone number in both lists, whereby the whitelist overrode the blacklist, and text messages from this number were allowed.



In our test, a newly entered number did not appear in the list immediately, only becoming visible when the list management had been closed and opened again.

BlackBelt could make some improvements here, and allow phone calls to be blocked too.

Wiping

This service allows the owner to send a command to the phone to initiate deletion of

the data on it. Wiping can be configured using BlackBelt Security's settings. The data to be deleted can be specified; by default, everything (SMS, contacts, mailbox, personal data and memory card) is deleted.

If the owner synchronises his/her contacts with a Google mail account, these will be globally deleted by an automatic synchronisation, as the account itself is not deleted. The continued existence of the account means that emails can still be read, received and sent.

After the deletion process, we were able to recover the majority of the data on our SD card with a recovery tool, in just a few minutes.

Ease of use

The graphical interface is kept very simple, and the help function provides appropriate assistance. We would suggest that user-friendliness would be improved by providing tool tips for all components, and adding a setup wizard. We were only able to discover that a remote wipe facility existed by consulting the help function. This component could be shown in the main menu, and configured from there.

Conclusion

BlackBelt Security is a well-designed security suite, which contains the most important protection components. Only a location function is missing. Some improvements could be made to the user-friendliness of the suite.

BlackBelt already started to work on the mentioned issues. In the improved version there is a complexity check of the password and the user is asked to carry out an initial update. Furthermore BlackBelt added a setup wizard and the product is no longer in yellow status following a successful installation. The problem concerning the Google account is also eliminated by deleting the password.

Furthermore BlackBelt integrated a location function and eliminated the black- and whitelisting problem mentioned above.

BullGuard Mobile Security

BullGuard Mobile Security is BullGuard's security product for mobile phones. It includes components such as antivirus, parental control, and backup.

Installation

The suite can be downloaded from BullGuard's website[2].

To download the software directly onto the mobile phone, the phone number has to be entered, and the button marked "Receive SMS now!" clicked. Unfortunately there is no confirmation that the request has been successfully completed, but a text message with the download link is subsequently sent.

An obvious plus point is that the phone's operating system is recognised automatically when clicking on the link, so the user merely has to click "Download".

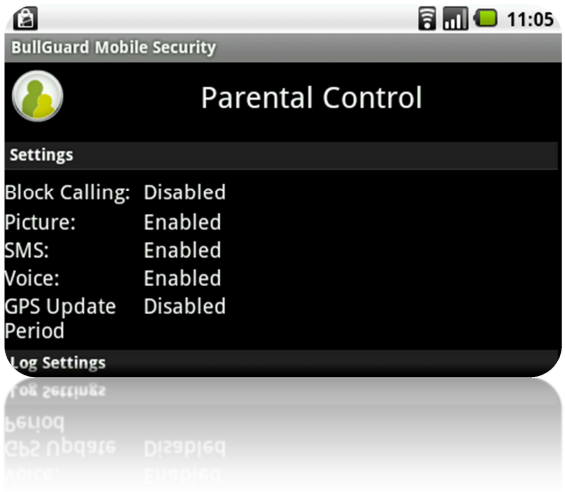
Starting the Program

After the first start, the licence agreement has to be accepted, and required information entered, such as the phone number with international code, licence key, email address and a password. The email address and password will be required later in order to log on to the web interface. After registration has completed successfully, an update is executed automatically.

AntiVirus

Parental Control

Although some components of parental control are shown on the phone as enabled, whilst others are shown as disabled, there is no means of changing the settings on the phone itself. All administration for the parental control component is carried out using the web interface, although this is not made clear in the phone software:

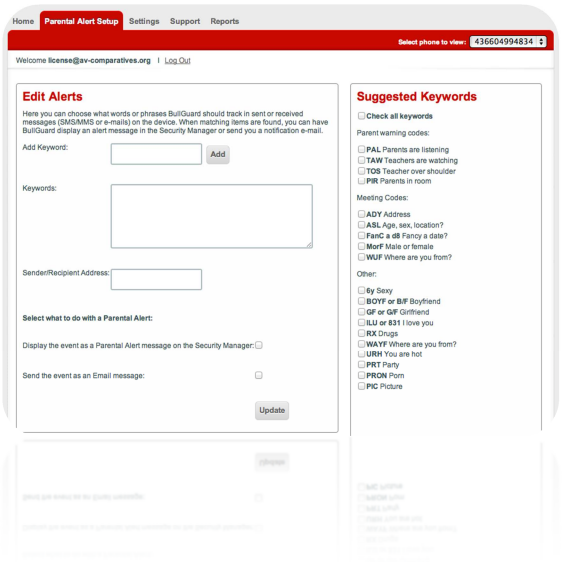


A message in the Parental Control status display, informing the user that all changes must be carried out via the web interface, would be very helpful.

Using the web interface, keywords can be added or selected from a list; Bullguard will then monitor the use of these keywords, in both sent and received messages. An email alert can be configured, so that the parent

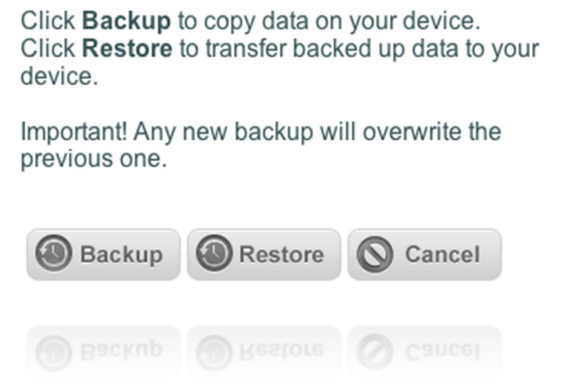
[2] https://www.bullguard.com/Mobile_v3/mobilesecuritydownload.aspx

can be informed when specific keywords are used.



Basic Backup

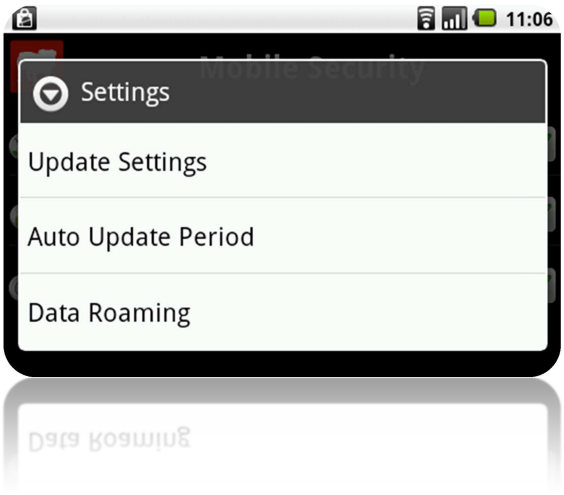
With the help of this service, the user can back up his or her contacts and calendar. This can also be done remotely using the web interface. This means that in the event of the phone beings stolen, the owner can back up the contacts and calendar remotely, before deleting the data from the phone.



The instructions for backing up shown in the screenshot above, namely "Click Backup to copy data on your device", is a little misleading. We would suggest "...back up your data to the cloud" would be clearer.

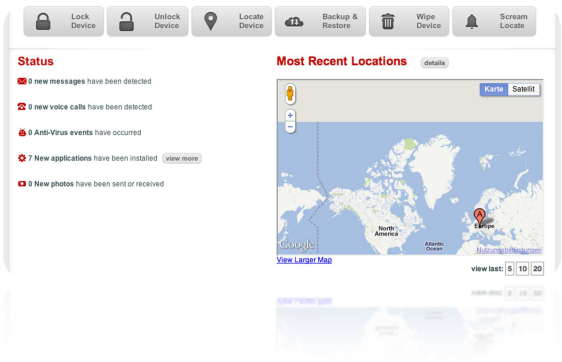
Settings

Under Settings, Data Roaming can be activated or deactivated, and automatic updates configured. Updates can be disabled completely, or set to run on a schedule, e.g. every 12 hours, every one or two days, every week.



In our test, we were unable to configure anything using Update Settings; it simply starts an update running, which is a little confusing.

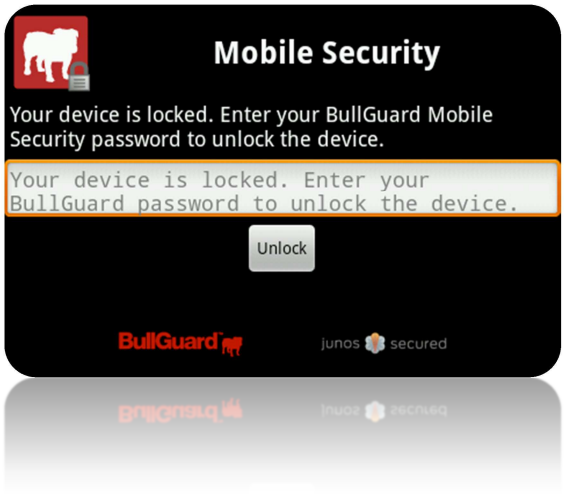
AntiTheft web interface



Unlike many other manufacturers, BullGuard uses a web-based interface for controlling its software. This means that theft-protection features such as Lock, Unlock, Locate and Wipe can be activated online. There is no need even to register a change of SIM card; as long as the application is installed, the device can be controlled through the web interface.

Lock Device

This feature enables the mobile phone to be locked with just two clicks. The web interface can be used to unlock the phone again (see below), or the phone can be unlocked locally by entering the password defined during installation.



Unlock Device

This allows a locked phone to be remotely unlocked.

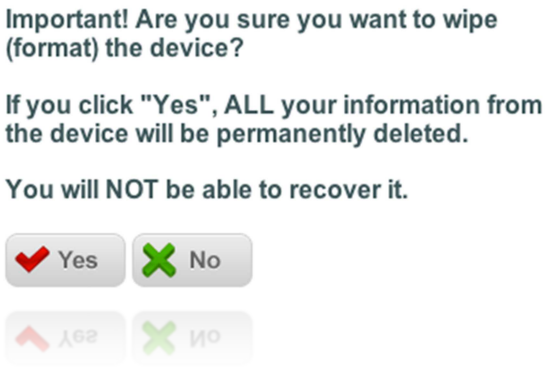
Locate Device

BullGuard offers a very simple means of finding out the current location of the phone, using its built-in GPS functionality. The web interface is used to send a "locate" command to the phone, which will send back its location if the GPS function is working. The location is shown on a map. In our test, this feature worked remarkably well, showing the location of the phone to within a few metres.

We must point out that a status message was received on our phone; this could alert a thief to the fact that the phone is being monitored, enabling him or her to deactivate the GPS function.

Wipe Device

BullGuard also has the ability to remotely delete data from the mobile phone. This service, like others, is controlled using the web interface. On our test device, the feature deleted all personal data such as the address book, pictures, call history etc.



However, the Google account was not deleted, meaning that emails could still be sent and received. An automatic synchronisation of our contacts also led to these being deleted globally.

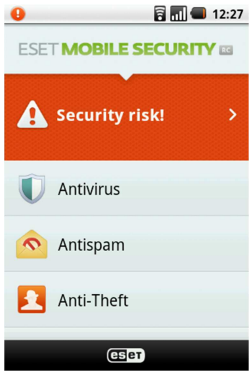
Using a recovery tool, we were able to get back all the deleted data from the SD card.

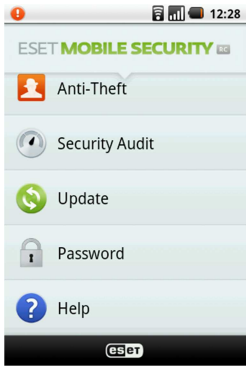
Conclusion

BullGuard Mobile Security appears at first to be a very cut-down security suite. Its full potential can only be realised by looking at the well-designed web interface; we suggest that there should be a reference to this interface in the mobile phone software itself.

ESET Mobile Security

The recently released version of ESET Mobile Security, which includes components such as Antivirus, Antispam and Anti-Theft, comes across as a well-designed and thought-out security suite.





Installation

We received the .apk setup file directly from ESET; we copied this onto an SD card, from which we were able to install it on our mobile phone without any difficulty.

Starting the Program

After installation, the licence agreement has to be accepted. We noted that the phone must be used in portrait format.

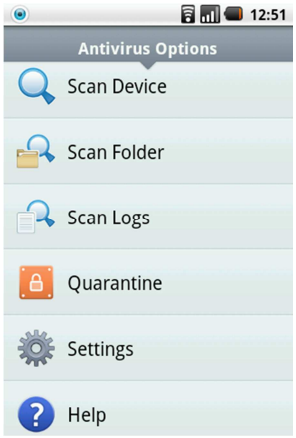
We were then struck by the warning "Security risk!". Opening the dialog box allows the user to necessary configuration steps to get rid of the warning message. These include SIM Matching, defining a trusted SIM card, and setting an ESET password.

We were particularly pleased to see that it is possible to decide for yourself when you want to be prompted for a password. Possible password-protected actions include opening the Antivirus, Antispam, Anti-Theft and Security Audit components, or uninstalling the security suite.

We chose to use a password for Anti-Theft, so that it can only be opened by entering the correct password.

Once all the necessary configuration changes have been made, the status display changes to "Maximum Security".

Antivirus

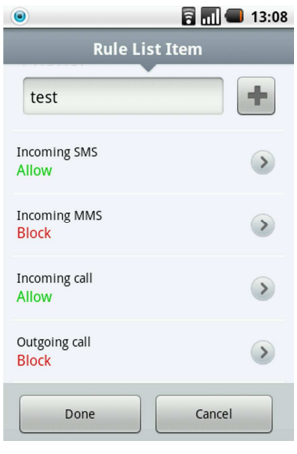


This component appears very highly developed, with all of the features found in ESET's antivirus software for home PCs.

It is possible to scan the entire device, or just individual folders, with the option of selecting specific file extensions to be checked.
The antivirus component has both on-demand and real-time protection, which can be configured as appropriate. For example, it is possible to configure the checking of applications, the display of warning messages, and what to do in the event of malware being discovered; the options are Ignore, Delete, Quarantine.

Antispam

This feature can be used to create rules for allowing or blocking incoming SMS and MMS messages, as well as both incoming and outgoing phone calls.



In the example shown here, the *test* contact can send SMS but not MMS messages to our phone; calls from the contact are allowed, but calls to

the contact are blocked.

Anti-Theft

For its Anti-Theft function, ESET, like many other manufacturers, uses text messages (SMS) to send commands. These commands are activated by default. The following options can be configured:

Trusted SIM cards

Trusted SIM cards can be defined. These are defined by the IMSI (International Mobile Subscriber Identifier). Multiple SIM cards can be added to the list.

If SIM matching is activated, and a non-trusted SIM card is put into the phone, ESET Mobile Security will lock the phone. In this case, a text message will be sent to any Trusted Friends (see below).

Trusted friends

Trusted Friends represent phone numbers to send warning text messages to in the event of a non-trusted SIM being put into the phone. A friend receiving such a warning message can reset the ESET password. When a non-trusted SIM is put into the user's phone a Trusted Friend can wipe the data or localize the phone and inform the owner about the situation.

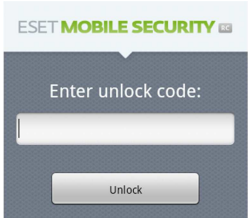
SMS Commands

This allows text message commands to be activated or deactivated. It contains a list of individual commands for locating, locking and wiping the phone.

Locating

To locate a lost or stolen mobile phone, a text message with the command *eset find [password]* (where *[password]* represents the actual password that has been configured) is sent to the phone. The sender then receives in return a link with the GPS co-ordinates for Google Maps, and a confirmation message.

Locking



To remotely lock the phone, the owner sends the phone a text message with the content *eset lock [password]*. The phone is then locked, and can only be unlocked by entering the password. The owner receives by return a confirmation message, with the IMSI and IMEI (International Mobile Equipment Identity).

Unfortunately, it is no longer possible to make emergency calls when the phone has been locked.

Wiping

The command *eset wipe [password]* can be sent to the phone to wipe personal data; the owner will receive a confirmation message. The phone's settings are then reset to factory defaults.

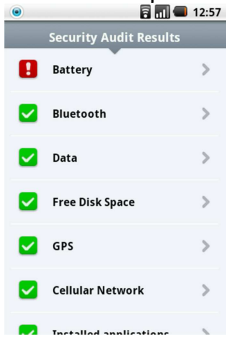
This meant that in our test, the Google account was also deleted, so the deletion of the contacts was not globally synchronised.
By using a recovery tool, we were able to restore much of the deleted data from the SD card.

Reset

We liked the ability to reset the ESET password by using a text command. This is done by sending a text from a phone number listed in the register of Trusted Friends (see above).

Security Audit

This component checks the security status of the mobile phone. The status of the battery, Bluetooth and GPS services, and applications is checked and displayed. Thus the user is made aware of any possible dangers, and can react appropriately.



Task Manager

Security Audit also contains a Task Manager, which shows running processes, services and tasks. Any non-system processes or services can be stopped using the applet.

Update

The schedule for automatic updates can be altered; username and password are actually not required to do this.

Password

The password can be reset with this function; the user has to enter the existing password first.

Help

ESET Mobile Security's Help function is very well structured and easy to understand. Every component is fully described.

Conclusion

ESET Mobile Security has developed enormously relative to last year's version. It is a very mature product, and can be likened to an antivirus program for a home PC. We were particularly impressed with the uninstall protection.

Public availability of ESET Mobile Security for Android is in October 2011.

F-Secure Mobile Security

F-Secure Mobile Security is a complete security solution. It includes features such as antivirus, theft protection, browser protection and parental control. The user interface has not changed since the last version, meaning that an upgrade does not involve any sort of reorientation on the part of the user.

Sicherheitsüberblick = security overview
Sie sind geschützt = you are protected
Aktualisiert = updated
Abonnement = subscription
Virenschutz = virus protection
Diebstahlsicherung = theft protecion
Einstellungen = settings

Installation

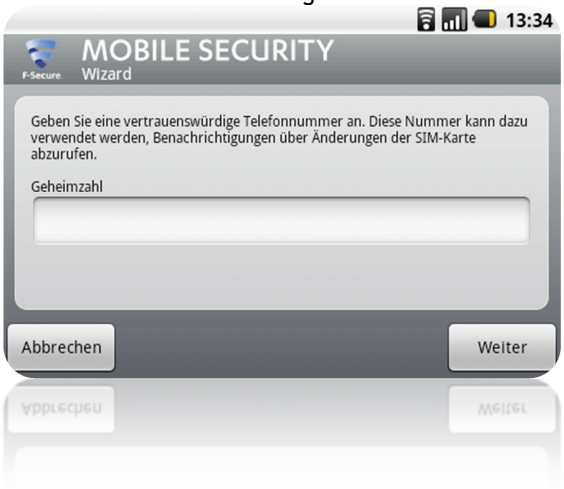
F-Secure Mobile Security 7.0 can be downloaded and installed directly from the F-Secure website[3]. The website offers versions for different operating systems, including Symbian, Android 1.6, 2.0, 2.1, 2.2, 2.3, and Windows Mobile.

Starting the Program

After the installation, the configuration wizard starts. The first step is to activate F-Secure Mobile Security. This involves accepting the licence agreement; rather confusingly, this is dated 2009. More confusingly, if you read the agreement and click the link "back to main page", you will be taken back to the licence agreement from 2008. We would suggest that there is room for improvement by F-Secure here.

Having got through the licence agreement, the user can choose between entering a licence key for the full version, or using a test version. The wizard then asks if the program should connect to its update server.

The next step allows the theft protection to be configured. A security code (password) has to be defined; this must be at least 5 characters long, and is checked for complexity. Mobile Security then requires the device administrator to be activated, in order to lock or wipe the phone, or reset the password, should the need arise.
Locking the phone may need to be configured in Android's security settings, as F-Secure does not have its own lock function, it just uses Android's. The next step requires a trusted phone number to be entered, which will be used to inform the owner in the event that the SIM card is changed:



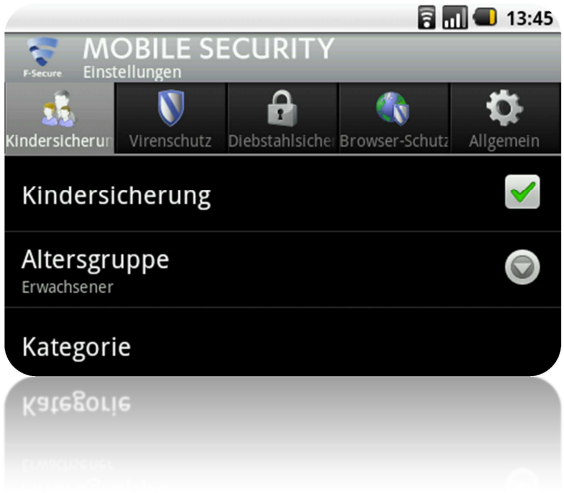
In the German version, the term *Geheimzahl*, literally "secret number", is used; we found this confusing, as the number to be entered is a trusted telephone number.

[3] http://mobile.f-secure.com

Once the trusted phone number has been entered, the user is asked to configure the parental control element. There are three age categories available: adult, teenager and child. F-Secure offers the ability to block Internet content that may be unsuitable for children.

Finally, a malware scan can be run.

Parental control



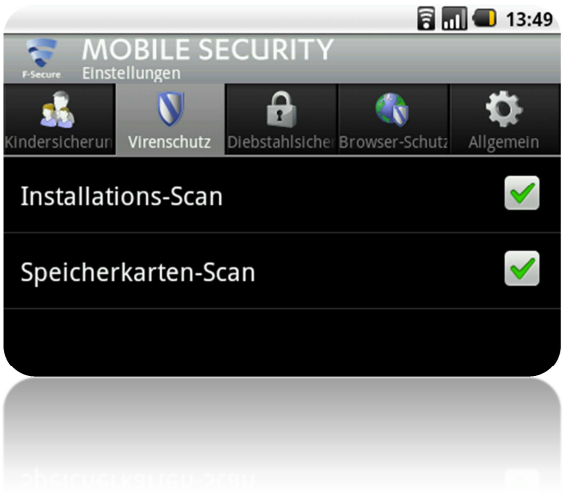
Kindersicherung = parental control
Altersgruppe = age group
Kategorie = category

The parental control component is activated by default. It can be configured in detail by allowing or blocking individual categories such as chat, webmail, weapons, and gambling for each age group.

Virus protection

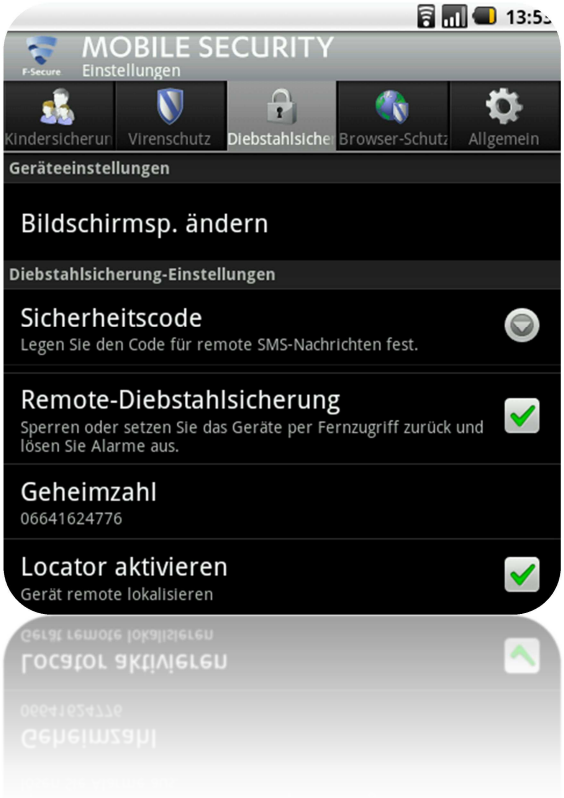
Scans of memory cards and applications (the latter run during installation) can be activated or deactivated here.

We would find a short description of the installation scan (and indeed other components and functions) very useful, and suggest that F-Secure should add this.



Speicherkarten-Scan = scan SD card

Theft Protection



Bildschirmsp. Ändern = change screen language
Sicherheitscode = security code
Remote-Diebstahlsicherung = remote theft protecton
Geheimzahl [incorrect German] = trusted phone number

Here, the user can change settings such as screen lock, security code, remote theft protection, and locator.

We were particularly pleased to note that every change to the theft protection features required the security code to be entered.

Screen lock settings

The screen lock can be changed via Android's security settings. It can be controlled using a passcode or Android's gesture function.

Security code

To change the security code, the old code must be entered once, and the new code twice.

Remote Theft Protection

Remote Theft Protection can be activated here by putting a tick (checkmark) in the relevant box.

Remote Lock

The mobile phone is locked by sending a text message with the content *#lock#[security code]* whereby *[security code]* represents the actual code that has been defined. The Android device lock (which can be unlocked by using a PIN or gestures etc.) is then activated. F-Secure's own security code is not used to unlock the phone.
Emergency calls can thus still be made even when the phone is locked, as the Android lock allows this. If the owner uses gestures to lock/unlock the phone, these can in many cases be determined by looking for oily marks left by the finger on the smartphone's touchscreen. The fact that gestures are frequently used, rather than the security code, makes it easier for the thief to determine what they are.

We feel that F-Secure might be able to offer a more secure locking/unlocking mechanism of their own, rather than using Android's. We would hope that doing this would allow the phone to make emergency calls.

Remote Wipe

Sending the remote wipe command (*#wipe#[security code]*) resets the phone to factory settings; this of course removes the F-Secure program from the phone. As a result, it will no longer be possible to use the security suite to locate the phone; on the other hand, as any Google account will also be deleted, there is no danger of an automatic synchronisation causing a global deletion of contacts.

It must be noted that with F-Secure too, it was possible to recover the deleted data from the SD card using an appropriate tool.

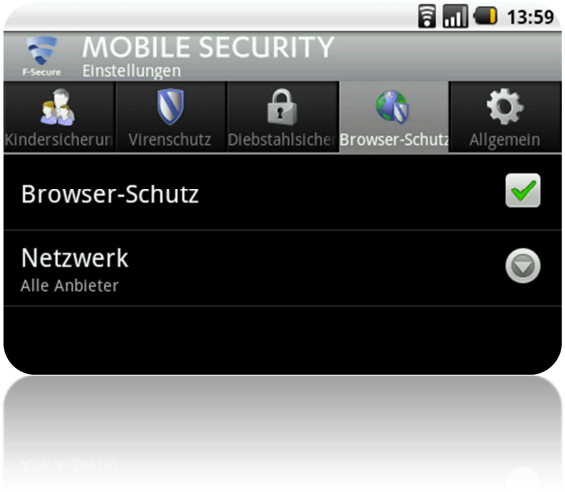
Trusted phone number

A trusted phone number, to which messages reporting a change of SIM card can be sent, is entered here.

Activating the locator

Activating the locator function allows the owner to locate a lost or stolen phone, by sending the text message *#locate#[security code]* to the phone. This results in a text message being sent to the owner with the GPS co-ordinates of the phone, which can be opened in Google Maps.

Browser Protection

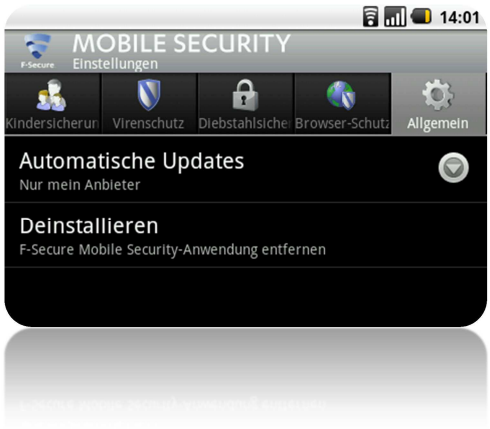


Browser-Schutz = browser protection
Netzwerk = network

F-Secure's browser protection feature is activated by default, for all network providers. It can be deactivated for specific providers if desired.

General

The last section allows the user to decide whether to download updates when connected to the mobile phone network by an alternative provider. By default, updates are only downloaded when the phone is connected via the user's own provider, to prevent high roaming data costs.



Deinstalliern = uninstall

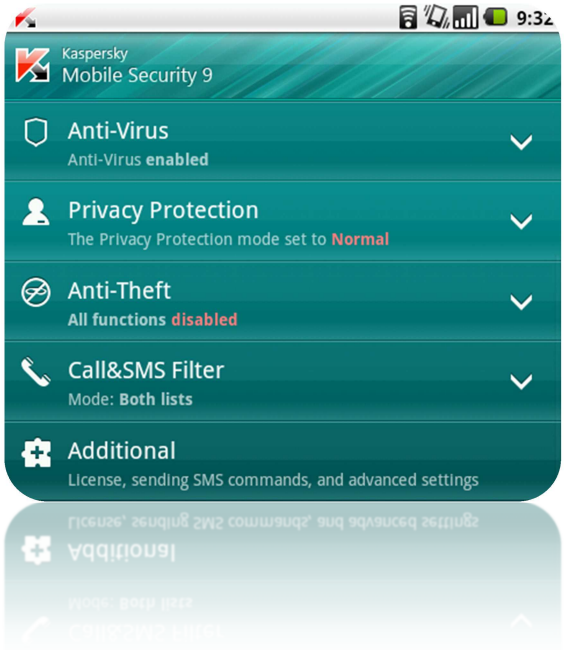
Conclusion

F-Secure Mobile Security provides the most important security components for a mobile phone. The well-designed configuration wizard allows even inexperienced users to set up the product successfully.

The phone lock feature was the only thing we felt F-Secure could improve; we suggest using the F-Secure's own security code instead of Android's.

Kaspersky Mobile Security

Kaspersky Mobile Security 9 offers users a security suite consisting of components such as Anti-Virus, Privacy Protection, Anti-Theft, and Call & SMS Filter. Kaspersky enhances the user interface with tool tips.



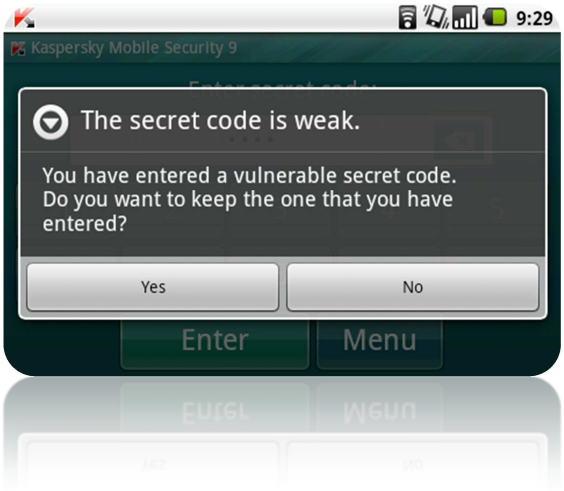
Installation

The installation of Kaspersky Mobile is carried out by downloading and installing from Kaspersky's website directly to the mobile phone.

Starting the program

After the first program start, there is a licence agreement to accept. There then follows the option to enter a licence key or use a trial version.

Having entered a licence key, we were then asked to enter a Secret Code, which Kaspersky requires to allow settings to be changed, or the phone to be unlocked. If a weak Secret Code is entered, the user will be informed (see below), although the warning can be ignored.



The next step allows the user to define an email address to use in the event that the Secret Code is forgotten. A message informs the user that a connection to the Secret Code Recovery Server will be made, meaning that data roaming charges may apply.

There was no automatic update or malware scan after the initial program start.

Anti-Virus

The real-time protection in Kaspersky Mobile Security is activated by default. The Anti-Virus feature allows the user to run a scan, and set options for this. These include file types to be scanned (all, or only executable), and action in the event of malware discovery (delete or ignore).

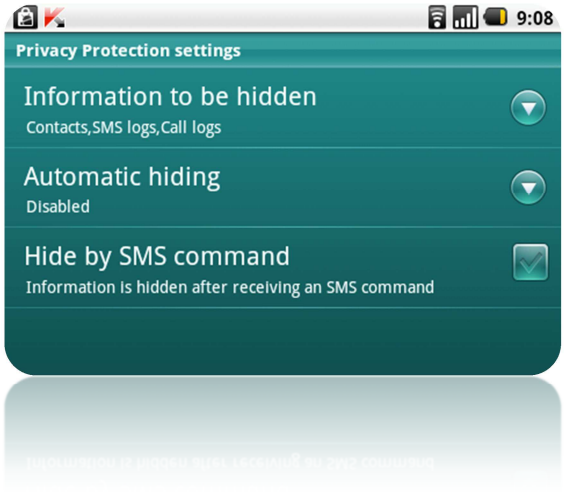
Automatic updates and scans can also be configured.

Privacy Protection

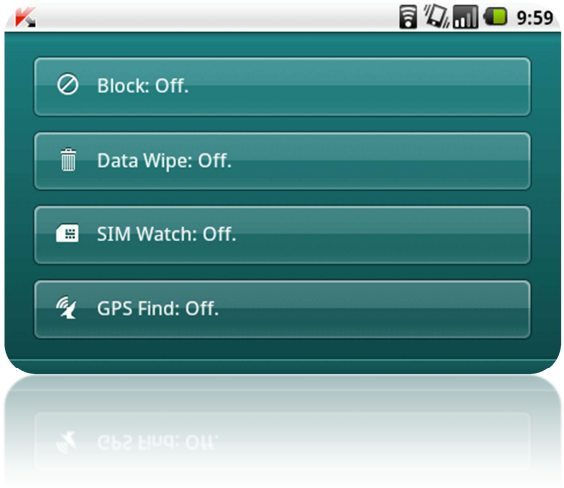
This component allows information and events relating to confidential contact entries to be hidden.

By default, the status is set to Normal, whereby nothing is hidden. In order to use the feature, the user has to add a number or name from the address book to the Privacy Protection contact list. Each entry can be configured in detail, so that individual items (such as SMS and call logs) can be hidden or shown.

The Privacy Protection feature can be remotely activated by text message.



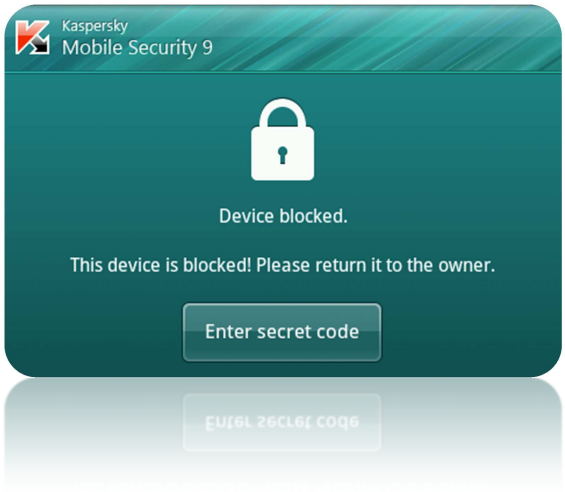
Anti-Theft



The theft protection feature of Kaspersky Mobile Security is turned off by default. Individual functions such as Block, Data Wipe, SIM Watch and GPS Find can be activated individually.

Kaspersky uses text messages to issue remote commands. If the appropriate function has been activated, text messages can be used to e.g. lock or wipe the phone.

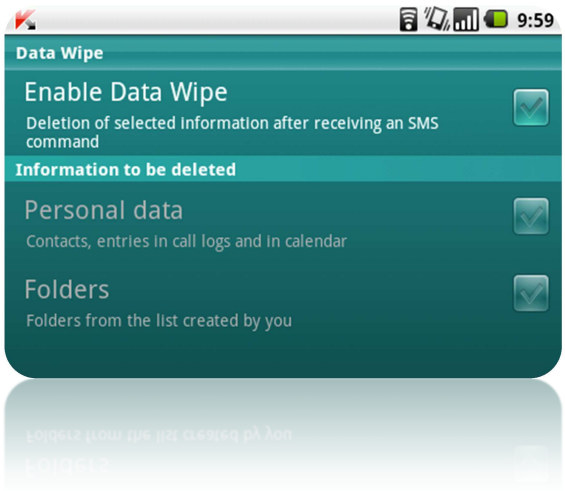
Block



If the Block function is activated, sending the appropriate command, *block:[secret code]* (whereby [secret code] represents the predefined entry) locks the phone's screen, as shown above. Only entering the Secret Code can unlock it.

In our test, we found it was impossible to make emergency calls, or to receive calls; the latter would make recovering the phone from an honest finder much more difficult.

Data Wipe



Sending the text message *wipe:[secret code]* results in the deletion of personal files and other user data from the phone.

In our test, the target data was successfully deleted, including the password for our Gmail account. This meant that mails and contacts could no longer be synchronised.

There was unfortunately one point to criticise: we were able to recover much of the deleted data from the SD card using an appropriate recovery tool.

SIM Watch

This feature automatically locks the phone in the event that the SIM card is changed. Additionally, the phone number of the newly inserted SIM card is texted to a pre-defined trusted telephone number, meaning that remote location and wipe features can continue to be used even with the new SIM card.

GPS Find

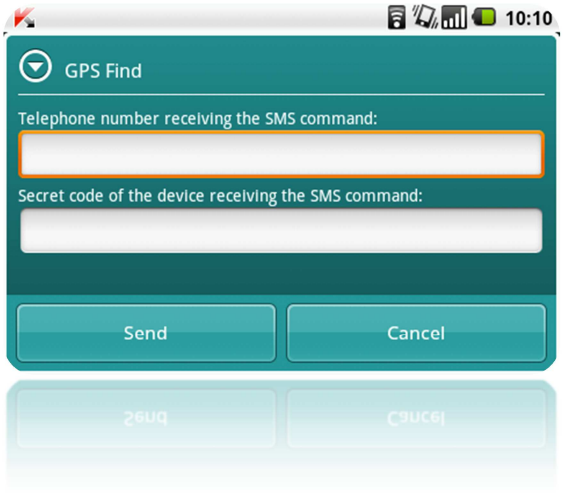
Kaspersky has also developed a useful tool for locating the phone if it is lost or stolen. If the user sends the message *find:[secret code]* to the missing phone, a return message containing the GPS co-ordinates will be sent to the sending phone and the email address defined during setup.

Call & SMS Filter

The Call & SMS Filter uses blacklists and whitelists to block unwanted calls and text messages. The telephone number can be used to screen out both calls and text messages, and keywords can be used as an additional filter for texts.

Additional

The last section allows alerts and information messages to be configured, and the Secret Code to be changed. Kaspersky has developed its own formula for sending SMS commands; the user selects the command to be sent, and then enters the phone number along with the Secret Code, which creates and sends the appropriate text message.



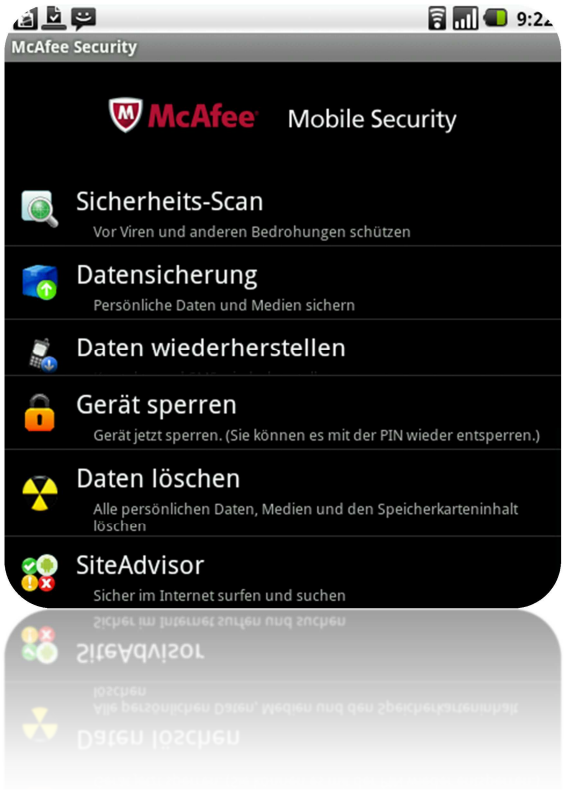
Conclusion

We found the Remote Wipe process in Kaspersky Mobile Security to be particularly good, as it does not simply reset the phone's state to the factory default. This means that even after a remote wipe, all functions of the security suite are still operating, and can be used to help recover the phone.

In our test, Kaspersky was the only product (apart from those that reset the phone to factory defaults) to delete the password to our Google account. This meant that the deletion of items from the phone was not automatically synchronised and thus globally deleted.

McAfee Mobile Security

McAfee Mobile Security enables users to configure their phones using a clear and simple web interface. Features such as security scanning, data backup, data deletion and recovery, device lock and web protection are included.



Sicherheits-Scan = security scan
Datensicherung = data backup
Daten wiederherstellen = restore data
Gerät sperren = lock device
Daten löschen = wipe data

Installation

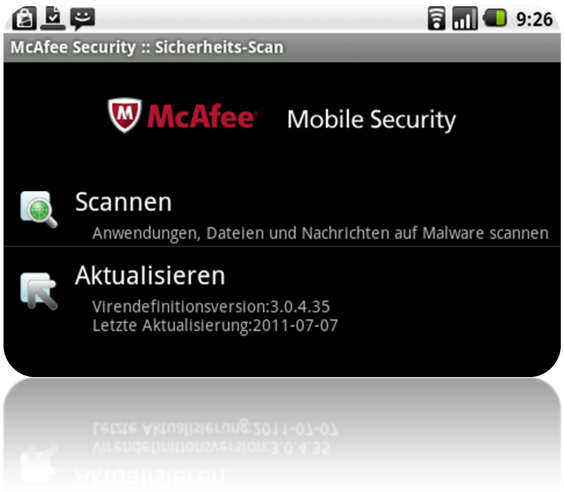
We downloaded McAfee Mobile Security from the Android Market and installed it without any difficulty; the German version was installed by default.

Starting the program

First the licence agreement has to be accepted. This is followed by registration of the program, which involves entering the phone number of the mobile phone (this is checked), an email address, a 6-digit PIN, and the number of at least one trusted person, who will be informed in the event that the SIM card is changed. In our test, a confirmation text was sent to the phone of our trusted person. Finally, the welcome screen is shown, with an overview of the suite's features.

After the installation and configuration process has been completed, there is no automatic update carried out, because in the downloaded package the signatures are already up to date. Our virus definitions were 9 days old.

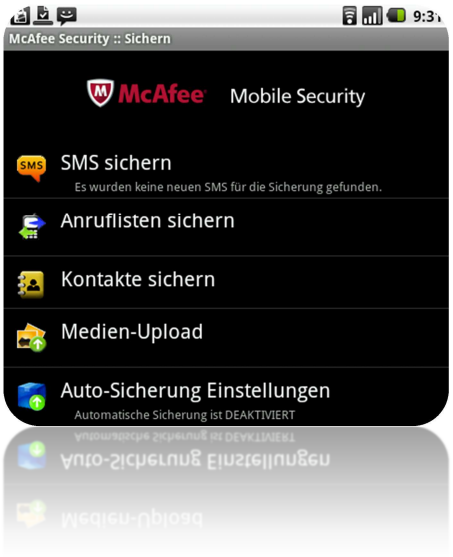
Security Scan



Scannen = scan
Aktualisieren = update

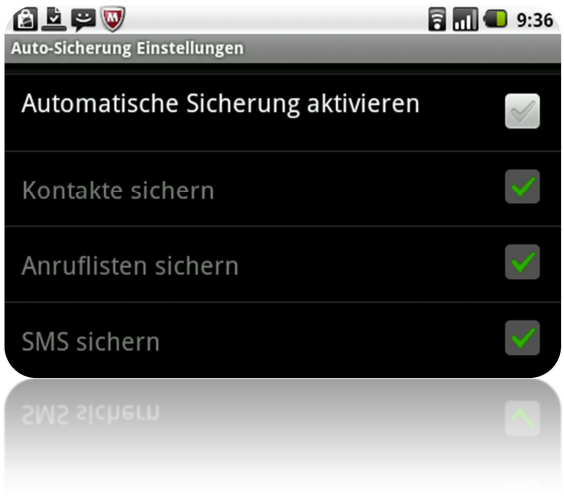
When this feature is first started, the user is asked whether to carry out an update. A scan can then be started using the appropriate button.

Data backup



SMS sichern = backup texts
Anruflisten sichern = backup call logs
Kontakte sichern = backup contacts
Medien upload = upload media
Auto-Sicherung Einstellungen = automatic backup settings

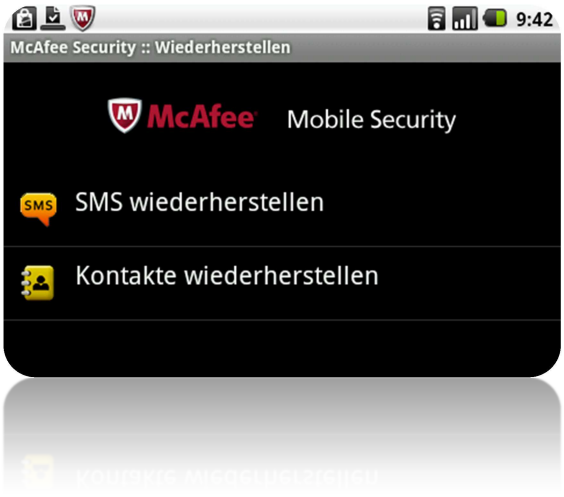
The data backup feature allows text messages, call logs, contacts and media to be saved to a remote server. We were pleased to note that only new text messages and contacts were backed up, meaning that no duplicates were created. Media backup allowed us to save all of our photos using the relevant menu.



Automatische Sicherung aktivieren = activate automatic backup

Automatic Backup is disabled by default. If activated, the feature will allow the daily backup of pre-defined data. In order to preserve battery life, this is only done when the phone is being charged.

Data recovery



SMS wiederherstellen = recover texts
Kontakte wiederherstellen = recover contacts

Using this feature, the user can restore backed-up text messages and contacts from the server. In our test, this functioned perfectly.

We were unable to find a way of restoring backed-up pictures and call logs, however, which was confusing.

Device Lock

The "Device Lock" button locks the mobile phone immediately.

Data Wipe

This function will, after confirmation of a warning message, delete all contacts, text message, call logs, photos, videos and the entire content of the SD card.

SiteAdvisor

SiteAdvisor offers safe surfing of the Internet. We are inclined to ask whether we are not protected by "normal" use of the browser, i.e. without SiteAdvisor. We feel McAfee should provide more information about what SiteAdvisor does.

Web Interface

Logging on to the appropriate website [4] enables the user to open the web interface of the software. This allows remote control of all the previously mentioned components.

Lock

This feature allows the phone to locked or unlocked remotely, and to set a lock with alarm.

McAfee Mobile Security, like many other products in this review, prevents the phone from being used to make emergency calls when it is locked.

When we locked the phone remotely in our test, a message was displayed with the telephone number that had requested the return of the device. It would seem ideal if this number could be called directly.

[4] https://www.mcafeemobilesecurity.com/default.aspx

Monitoring

In the event that the SIM card in the phone has been changed, the owner can see the new number here.

Location

Location is a very useful feature, although one that needs to be used with care. It can be used to locate the mobile phone of the owner's child or partner; the current location is shown on a map. Real-time monitoring, which notes the location every hour for 6 hours, can also be started here.

Backup

We could not find any difference here relative to the controls on the phone itself, though of course the ability to back the phone up remotely before wiping is very valuable.

Data wipe

In contrast to the locally started wipe process, the web-based interface gives the owner the choice of which data should be deleted:

Speicherkarte = SD card
Anruflisten = call logs

Contacts, text messages, photos, videos, call logs and the content of the SD card can be selected and deleted.

After successfully completing a data wipe, we found that McAfee Mobile Security, like many other products, had not deleted our Google account. It was possible to read, send and receive emails. Synchronising the account led to global deletion of the contacts.

We were also able to recover the deleted data from the SD card using an appropriate recovery tool.

Restore

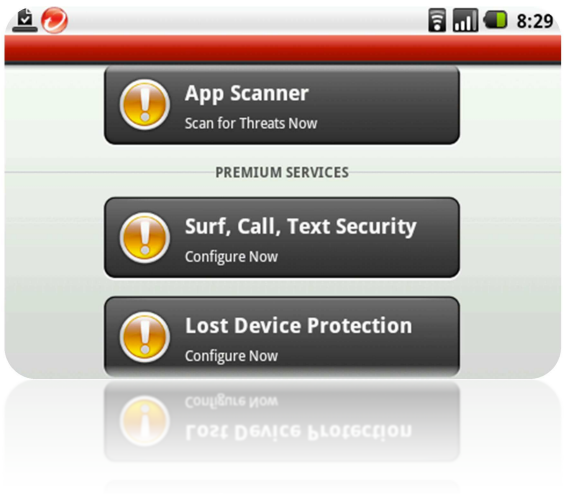
A message is displayed, stating that data has to be restored using the phone itself, rather than the web interface; this makes sense.

Conclusion

McAfee Mobile Security is a well-designed security suite, which offers a very user-friendly backup feature. Why this allows the backup of pictures and call logs, but offers no way of restoring them, remains a mystery to us.

Trend Micro Mobile Security

Trend Micro Mobile Security Personal Edition 2.0 is Trend Micro's security suite for mobile phones. It includes App Scanner, Surf-Call-Text Security, and a theft protection module. A web interface can be used to send commands to the phone if necessary.



Installation

Trend Micro Mobile Security Personal Edition can be downloaded and installed directly from the Android Market.

Starting the program

When first starting the program, the user has to create a Trend Micro user account, or give the credentials of an existing one. If creating an account for the first time, there is a licence agreement to accept. To configure Mobile Security, the user has to enter an email address, password, first and last names, and a location. The password has to be between 8 and 50 characters long.

We noticed that there was no automatic update carried out on completion of the registration process. We did however receive a confirmation email with information relating to the use of the web portal with the theft protection feature. In order to activate all of the features of the suite, we entered an activation key via the main menu. There is also the opportunity to buy a key if necessary.

App Scanner

The App Scanner checks installed applications for security risks. By default, real-time protection and automatic updates are activated, although the user can deactivate and reactivate them if desired.

Surf, Call, Text Security

This section allows Safe Surfing, Parental Controls and Call/Text Blocking to be configured.

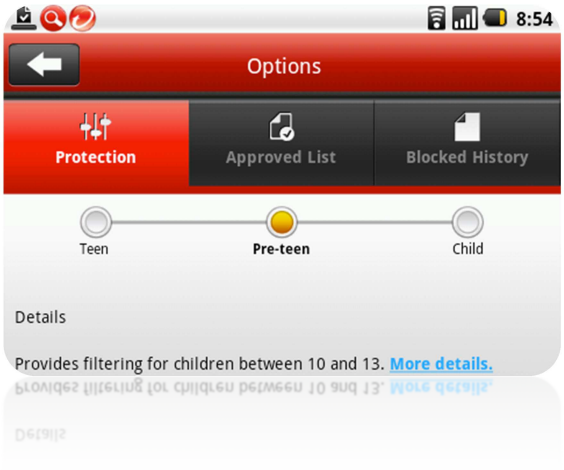
Safe Surfing

This component is activated at "normal" level by default.

Via the three buttons, Safe Surfing can be set to Low, Normal or High. The approved list can be used to allow specific websites which would otherwise be blocked under the current policy.

Parental Controls

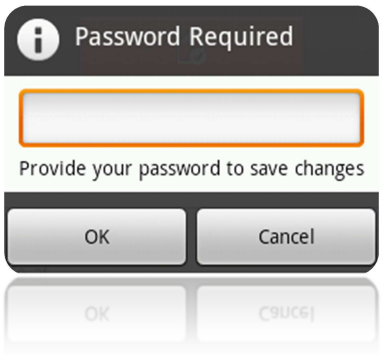
Parental Controls is not activated by default. The password has to be entered in order to enable it. The default protection level is Pre-Teen (the middle setting), with Teen and Child as alternative options. Selecting a particular level shows details of the age group it is aimed at (Pre-Teen being 10-13), with a link to further details provided.



There is also the opportunity here to add specific websites to the Approved List,

meaning that they can be seen, even though the default policy would block them.

A password is demanded here, although we were able to edit entries even when we entered the wrong password or no password.



Call Blocking

This component allows the user to block unwanted calls. Telephone numbers can be manually entered, or selected from the address book, call log or SMS list, and added to either the Blocked List or Approved List.

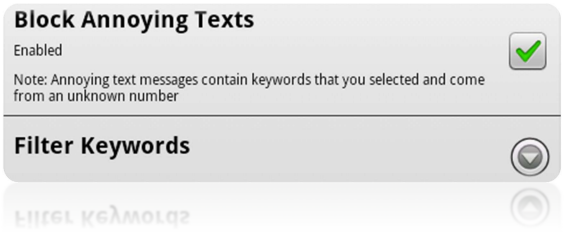
There are two methods of filtering calls available: all calls are allowed, unless the caller is on the Blocked List; or all calls are blocked, unless the caller is on the Approved List.

There are three possible courses of action for calls blocked by either method: Reject Call; Silence Device; Reject Call + Send Reply.

A final option is Block Annoying Calls, which is disabled by default. This blocks calls from unknown numbers within three seconds.

Text Blocking

Text Blocking works in much the same way as Call Blocking. It allows texts from specific senders to be blocked, and can also block texts on the basis of pre-defined keywords in the message. To use this feature, it has to be activated, and the relevant keywords entered.



Lost Device Protection

Trend Micro Mobile Security Personal Edition contains the following components, each of which is explained by a short help text in the program.

Locate – Find My Android

This component locates a lost mobile phone using GPS or WiFi. It is activated by default, and can be switched off or on from the phone itself.

Scream

This can be used to set off an alarm in the phone when it connects to the internet. The feature is controlled from the web portal.

If the device lock has not been activated, there is nothing to prevent the finder switching the feature off. It might be better to automatically lock the phone first, in order to prevent this happening.

In our test, the alarm went off even when the phone was set to silent.

Lock – Remote Lock

The lock function locks the mobile phone when it connects to a wireless network (WiFi). This function can be controlled via the web portal. On the device itself, it is possible to change the dialog box that is shown when the phone is locked.

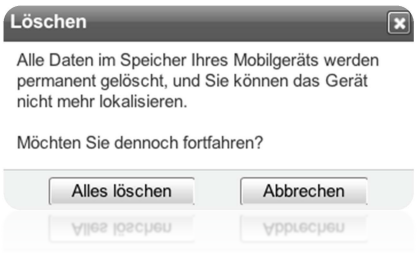
By default, the following message is shown when the phone is locked:

In the provided product, we have been able to unlock the phone using any password or even no password. This issue is solved in the current version.

Remote Wipe

The wipe function can be used to delete all personal data from a lost or stolen phone, using the web portal. An internet connection is required.

Selecting Remote Wipe in the web portal brings up the following warning message:



Delete
All data on your portable device will be permanently deleted, and you will no longer be able to locate the device.
Do you want to proceed?
Delete All | Cancel

Choosing "Delete All" resets the phone to factory defaults. This deletes the Google account, meaning that contacts cannot be globally deleted by automatic synchronisation.
With a recovery tool, we were able to get back most of the data from the SD card.

SIM - SIM Card Lock

As soon as the original SIM card is removed, the phone is locked automatically. This feature can be switched on or off from the phone itself.

Web portal

Features such as Find My Android, Remote Locate, Remote Lock, Remote Wipe and Scream are configured by logging on to the website[5] portal.

There are buttons for each of the functions above, and a map showing the phone's location.

Conclusion

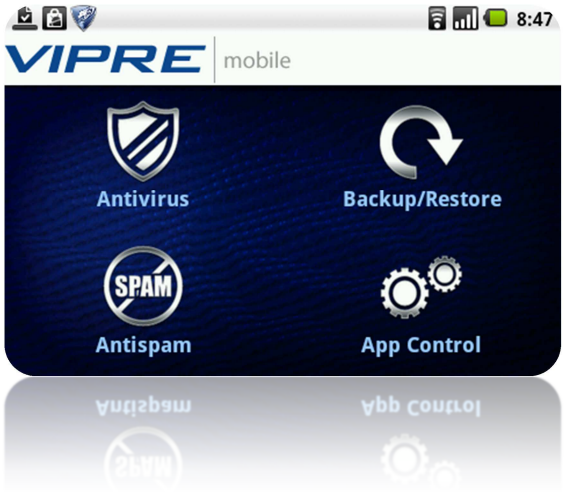
Trend Micro Mobile Security gets high marks for its clear, uncluttered interface, and easy configuration of all the individual components. The help function explains every detail of the program clearly.

The complete ineffectiveness of the password protection mechanism, i.e. the password prompt allowing access with any or no password, is a serious failing, which must be rectified urgently.

[5] http://www.trendmicro.com/ILostMyAndroid

VIPRE Mobile Security

VIPRE Mobile Security is made by GFI Software, and was in beta stage at the time of our review. The phone interface is very simply designed, the full range of features being more easily visible in the web interface.



Installation

Vipre Mobile Security can be downloaded and installed directly from the Android Market. In our test, installation was quick and unproblematic.

Starting the program

When the program is first started, there is a licence agreement to accept. An easy-to-use wizard then leads the user through the configuration process.

The first step is to create an account with GFI Software. An email address, password and device name have to be entered. The complexity of the password is not checked, we were able to use just 3 characters for ours.

If the user already has an account, this can be used to log on with, in which case the system asks whether the device should be restored from a backup.

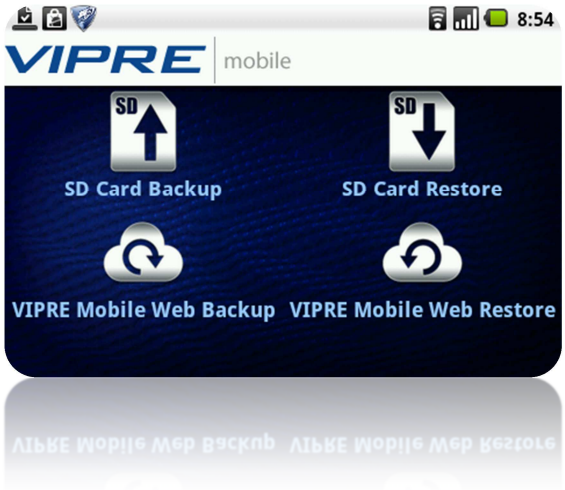
Finally, the Device Administrator has to be activated. This enables the Vipre suite to wipe the phone, reset the password etc.

In our test, a definitions update was carried out automatically when the wizard had finished.

Antivirus

This button allows a virus scan to be started. When scanning, the program will display the expected time to completion, and the icon changes to show details and progress.

Backup/Restore



This feature allows the user to back up personal data onto an SD card or a VIPRE backup server, and to restore from these sources.

SD Card Backup

Contacts, music, podcasts, ring tones, alarms, messages, pictures, videos, downloads and applications can be saved to the SD card. The user can save all of these categories or select them individually. Having made the selection, the user can start the backup using the menu or the Play button. We noticed that the Play button remains grey all the time, and could easily be overlooked; we would suggest that changing its colour when a selection is made would be helpful.

SD Card Restore

SD Card Restore allows data to be restored from a previous backup on the card.
Again we would like the grey Play button to change colour when a selection is made. When only one backup was available, it was impossible to deselect this once it had been selected.

VIPRE Mobile Web Backup

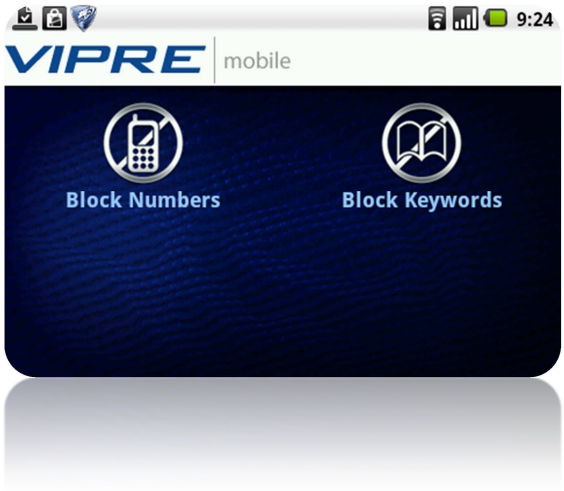
This tool backs the data up to a VIPRE server rather than a card. When it has been run, the backed-up data can be seen using the web interface.

VIPRE Mobile Web Restore

This allows backed-up data on the VIPRE server to be restored to the phone. Again, individual categories can be selected.

Antispam

Antispam is deactivated by default, and requires the entry of username and password to be activated or configured.



As with many other mobile security products, telephone numbers and keywords to be blocked can be specified.

Block Numbers

This feature allows phone numbers to be defined, to which *outgoing* calls cannot be made. We found this irritating, as most people want to block *incoming* calls from particular numbers, but incoming calls to the blocked numbers still come through. We would suggest that this feature cannot be described as antispam, it is much more a child protection feature, and so should be included in that section of the interface.

As it is outgoing calls that are blocked, it makes sense that phone numbers cannot be imported from the address book.

Block Keywords

In contrast to blocking calls, the Block Keywords feature relates to *incoming* messages. Defining keywords blocks incoming messages containing these words, but has no effect on outgoing messages.

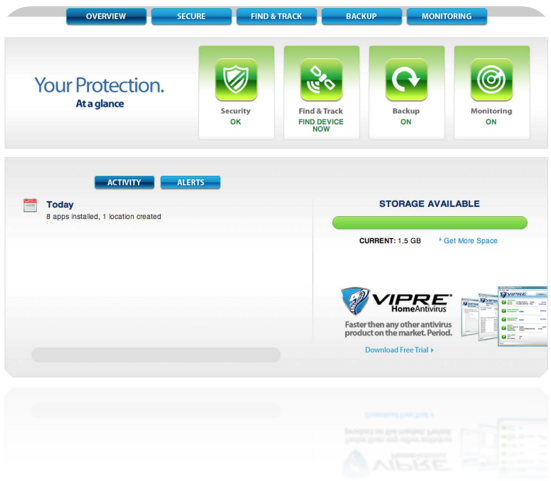
App Control

This component is also deactivated by default, and the password must be entered to enable it. The feature allows the user to password protect certain applications. There is also a second use, which we found most surprising: it allows you to decide which applications can be run whilst driving a car. We assume that the phone uses the built-in GPS to sense rapid movement. In any event, we suspect that many road safety campaigners will not regard this as a useful feature.

Wipe/Unlock

This feature is only accessible from the VIPRE menu, and is activated by default. The password is not required to switch it on or off. It can only be executed via the web interface.

Webinterface



Once the application has been installed, and an account created, the user has control over all mobile phones registered to the account, via the web interface. This is very intuitive and could easily be operated by any user.

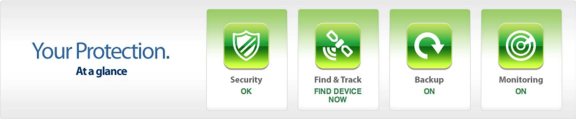
Straight after registration, all components are set to "off", but after a few minutes, we were able to configure all of them to provide the

best possible protection. A mini-tutorial would be helpful here, especially for less-experienced users.

There are five main areas to the web interface:

Overview

This shows the status of the individual components at a glance.

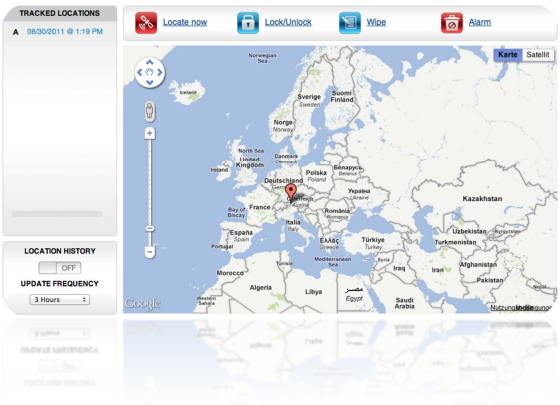


Secure

The Antivirus, Antispam and App Control components are configured here. For example, controls for the blacklists of keywords and phone numbers, the password for applications, and the update status are shown here.

Find & Track

Find & Track enables the owner of the phone to locate, lock/unlock or wipe the phone if it is lost or stolen; an alarm can also be set off.



Locate now

If a lost phone is successfully located, the its position will be shown on a map. In our test this worked perfectly, even showing the house number of the street.

Lock/Unlock

We were pleased to see that a separate password (Lock Code) can be used to temporarily unlock the phone when the Lock command has been sent remotely. After a certain period of inactivity, the phone will re-lock itself, and the Lock Code must be entered again. The phone can only be permanently unlocked by using the web interface (the Lock Code is not needed to do this, only the normal web interface credentials).

Wipe

With just a few clicks, the owner can delete all personal information from the phone. There is no choice of elements to be deleted, as the phone is simply reset to factory settings. Consequently there is no danger of the Google contacts being globally deleted via synchronisation with the phone.

We were able to restore all the wiped data from the SD card using a recovery tool.

Backup

This component allows the user to see his/her backed up data, and change it or delete it.

Monitoring

In the last section, Monitor, Parental Control, Antisexting and Antibullying can be configured. The Monitor can watch call logs, SMS & MMS, emails etc. Logs can be made of phone activities.

Parental Control can be used to set time limits for emails, Internet browsing, phone calls etc.

Antisexting and Antibullying allows keywords to be entered in a blacklist; any incoming messages containing these words will be blocked.

Conclusion

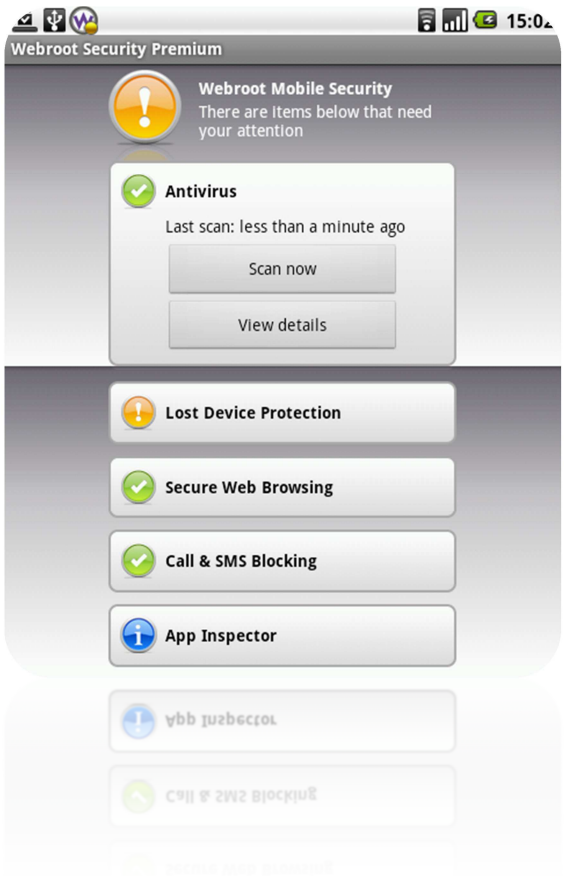
VIPRE Mobile Security is a clear and easy-to-use security product. The user is never overwhelmed with the range of configuration options.
The web interface is a simple and effective means of configuring the suite, although there is some room for improvement; for example, it takes some time for the initial

status warning to disappear and all components to be shown as “green”.

VIPRE Mobile Security is still undergoing some usability testing to further enhance the usability of the product.

Webroot Mobile Security

Webroot Mobile Security offers functions such as Antivirus, Lost Device Protection, Secure Web Browsing, Call & SMS Blocking, and App Inspector. The Lost Device Protection features can be used via an intuitive web interface or by sending text messages to the lost/stolen phone. Webroot Mobile Security is the only product in our review to offer both methods.



Installation

The free version of Webroot Mobile Security can be downloaded and automatically installed from the Android Market. For our test, we activated the Premium version with a licence key after installation.

Starting the program

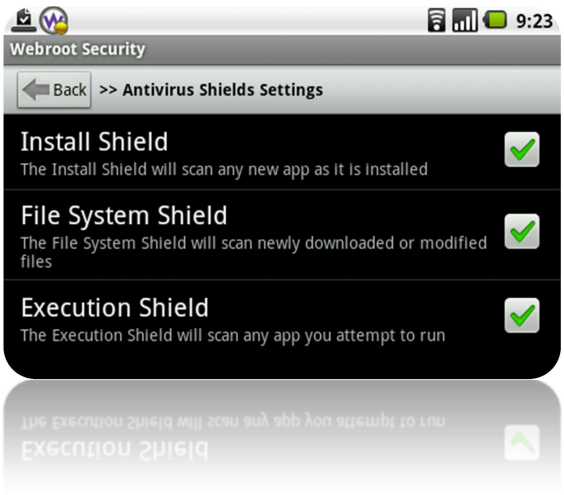
When starting the program for the first time, the licence agreement has to be accepted. The user then has to set up an account with Webroot, or log into an existing account.

For a new account registration, the user needs to enter an email address, a password with at least 6 characters, and the phone number of the mobile phone. In our test, the password was only checked for length, not complexity.

When the post-installation configuration has been completed, the phone is scanned for malware. The program then points out areas that need attention. We had to deactivate the option "Allow non-Market applications" in the device settings in order to obtain the "all clear" (green tick) from the antivirus component. To set the overall Webroot status to green, we had to activate Lost Device Protection.

Antivirus

This component is activated by default and allows the user to scan for malware set up special configurations.



The user has the option of activating or deactivating specific shields, which scan applications when installed or run, and scan every downloaded file.

It is also possible to set up scheduled scans and updates, which can be run hourly, weekly or monthly.

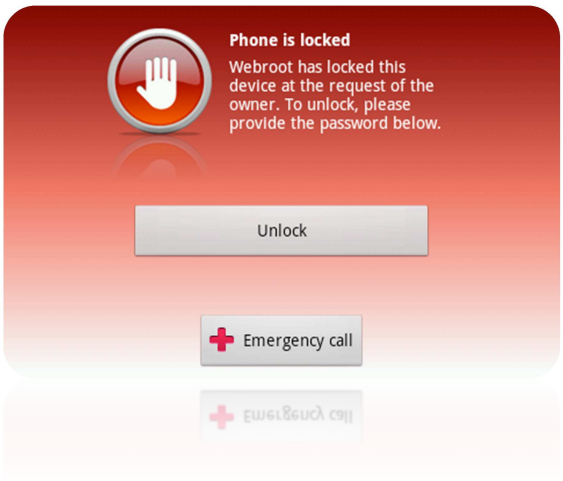
Lost Device Protection

Lost Device Protection is deactivated by default. It integrates the most important features for protecting private data in the event that the phone is lost or stolen.

The following features can only be used if Lost Device Protection is activated.

Lock

To lock the mobile phone remotely, the web interface can be used, or a text message sent to the phone with the content *lock [password]*. The lock screen shown below then appears on the phone; as can be seen, it is still possible to make emergency calls.



Locate

To find out the current location of the phone, the owner simply sends a text message from any SMS-capable device to the phone, with the message *locate [password]*. A text message will be sent by return containing the GPS co-ordinates; the lost phone will also be locked as soon as the *locate* message has been received.

The web interface can also be used to locate a lost phone; the location will be shown on a map.

A parent using this function to locate their child should note that the child will be unable to use the phone without using the password to unlock it.

Scream

If the user sends the text message *scream [password]*, the phone will be locked, and also emit a loud alarm signal; this sound can enable the user to locate the phone if it is lost, but will also deter the thief from carrying the phone around in public. The function can also be initiated from the web interface.

Wipe

The wipe command, *wipe [password]* (can also be sent from the web interface), deletes all personal data from the phone. In our test, all the data was deleted, although it was possible to recover a majority of the data on the SD card using a recovery tool. The password for the Google account was deleted, meaning that contact data could not be globally deleted by synchronisation from the phone.

SIM Card Lock

SIM Card Lock will lock the phone if the SIM card is removed or changed. This feature and Wipe are not available in the free version.

Secure Web Browsing

Secure Web Browsing allows the user to edit the list of websites classified as dangerous. It includes a log of sites the user has visited in spite of a warning that they may be risky.

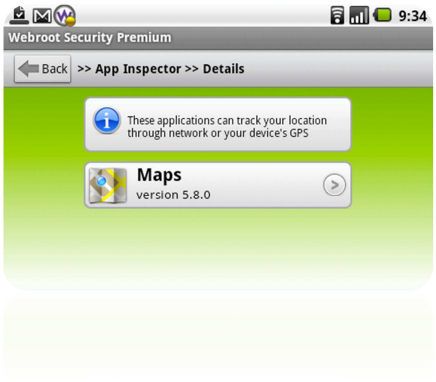
Call & SMS Blocking

This feature allows calls from specific numbers to be blocked, and SMS messages with suspicious links to be filtered out. It would appear to be very useful in the event of the phone's owner being stalked. We tested the call block by adding a number to the list, then calling the test phone from this number; the call was successfully blocked. The incoming call was displayed very briefly on the screen and then dropped. We suggest that Webroot might like to find a way to block the call without the caller having any indication

that this has happened, i.e. giving the caller the impression that the phone is simply switched off.

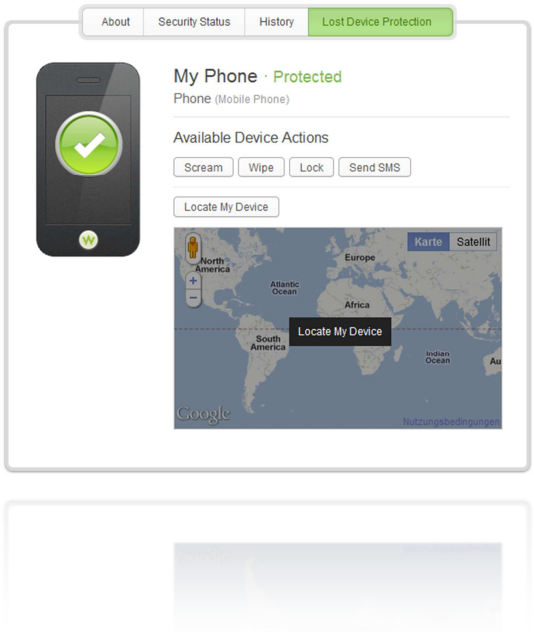
App Inspector

The last component of the suite is App Inspector. When it is run for the first time, an application scan is carried out. The result is potentially risky applications being assigned to one of four groups: Access Your Messages; Cost You More Money; Access Sensitive Information; Track Your Location.



Web Interface

Webroot Mobile Security users can control the theft protection features via the web interface. This is clearly and simply laid out, and provides information about the phone, licence key, security status, and logs.



The most important element is the theft protection, however. This enables the phone's owner to lock, wipe and locate the phone, or set off an alarm. It is also possible to send an SMS directly to the phone.

Conclusion

Webroot is the only product to offer controls by both SMS and web interface. We would however suggest that the web interface should be mentioned in the phone software, so that users are aware that it exists. It only came to our attention when reading the feature list.

Conclusion

In current times, nobody who has a smartphone should do without a security program for it; not only because of the risks of encountering malware on the Internet, but also – indeed especially – due to other threats, such as theft or data loss. Every smartphone, whether used for business or private purposes, should be protected.

All the products we tested were fit for purpose, but it is difficult to say which product is best suited to which user.

We did not notice any reduction in performance as a result of installing any of the products in our test. We did find that the time needed to charge the battery slightly increased, however.

In our opinion, all manufacturers should consider providing both web-based and text-message-based methods of using the theft protection features. Each has its own advantages and disadvantages; the web-based interface requires an Internet-connected PC, while the text commands require the use of another mobile phone, and the owner of the lost phone needs to remember the relevant commands to send.

We also feel that manufacturers must improve the data wipe function of their products, as in all cases it was possible to recover at least the majority of the data from the SD card after it had been remotely wiped.

Potential smartphone security software customers should consider carefully what their requirements are before purchasing. Almost all products are available to download as a free trial version. We would recommend that any smartphone security program should contain a minimum feature set of antivirus, phishing filter and remote lock.

Appendix A - Featurelist

Android									
	Blackbelt	Bullguard	ESET	F-Secure	GFI	Kaspersky	McAfee	Trend Micro	Webroot
Product name:	BlackBelt Security	BullGuard Mobile Security	ESET Mobile Security	F-Secure Mobile Security	VIPRE Mobile Security	Kaspersky Mobile Security	McAfee Mobile Security	Trend Micro Mobile Security Personal Edition	Webroot Mobile Security
Supported OS versions:	1.5 and above	2.0 - 2.3	2.0 - 2.3, 3.x experimental	1.6 - 2.3, 3.x	2.2 and above	1.6 - 2.3	2.1 and above	2.2 and above	2.1 and above
Supported Program languages:	English, French, Spanish, Traditional Chinese, Vietnamese	English	English, Polish, Danish, Finnish, Norwegian, Japanese, Russian, Hungarian, Estonian, German, Portuguese Brazilian, Dutch, French, Romanian, Turkish, Swedish, Chinese Simplified, Chinese Traditional, Italian, French Canadian, Korean, Spanish Latin, Czech, Hebrew, Slovak	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	English	English, Russian, German, French, Spanish, Italian, Dutch, Danish, Norwegian, Finnish, Swedish, Portugese, Brazilian Portugese, Polish, Turkish	English, Chinese Simplified, Chinese Traditional, German, French, Italian, Japanese, Dutch, Spanish, Portuguese, Brazilian Portuguese, Bahasa Indonesia, Korean, Swedish, French (Canadian), Spanish (Mexican), Russian, Norwegian, Danish, Finnish, Greek	English, Japanese, German, French, Italian, Spanish, Russian, Dutch, Brazil-Portuguese, Simplified Chinese, Traditional Chinese, Korean.	English, Japanese
Locking Features:									
Lock Contacts	●	-	-	●	●	●	●	-	●
Lock Images/Files	●	-	-	●	●	●	●	-	●
Lock SMS/MMS	●	-	-	●	●	●	●	-	●
Lock SIM	●	-	-	-	-	-	●	-	●
Anti Spam Features									
Whitelist/Blacklist calls	-	-	●	-	●	●	-	●	●
Whitelist/Blacklist SMS	●	-	●	-	●	●	-	●	●
Whitelist/Blacklist MMS	●	-	●	-	●	-	-	●	●
Block known SMS/MMS spam	-	-	-	-	●	-	-	●	●
mark as spam with one click	●	-	-	-	-	●	-	-	-
White- and Blacklisting with wildcards	●	-	-	-	●	●	-	-	-
Block attachments/applications/file extensions	-	-	-	-	-	-	●	-	-
Parental Control									
Pay Number locking	-	-	●	-	-	-	-	-	-
SMS Find (Localization of the Smartphone)	●	-	●	●	●	●	●	-	●
Log visited URLs	-	-	-	-	●	-	●	●	-
Firewall Features:									
App Whitelisting/Blacklisting	-	-	-	-	●	-	-	-	-
Different protection level	-	-	-	-	●	-	-	-	-
Activity log / Protection log	-	-	-	-	●	-	-	-	-
Remote Features									
Remote wipe of a stolen Smartphone	●	●	●	●	●	●	●	●	●
Remote GPS localization	●	●	●	●	●	●	●	●	●
SIM Watch (changing the SIM)	●	●	●	●	-	●	●	●	●
Remote installation of the Security System	-	-	-	-	●	●	-	-	-
Remote configuration	-	●	-	●	●	●	●	●	-
Remote updates	-	-	-	●	●	●	●	●	●
Central Management	-	●	-	●	●	●	●	●	●
Authentication									
Policy controlled authentication	-	-	-	-	-	-	-	●	-
Access control	-	-	-	●	-	-	●	●	-
Password policy: Strength, length, etc.	-	-	-	●	-	●	●	●	-
Maximum number of failed attempts	-	-	-	●	-	-	-	-	-
Grace period	-	-	-	●	-	-	-	-	-
Lock Screen with Password protection	●	●	-	●	●	●	●	●	-
AV Features									
Real Time File protection	●	●	●	●	●	●	●	●	●
On Demand Scan	●	●	●	●	●	●	●	●	●
Network protection	●	-	●	-	-	●	-	-	●
SMS/MMS Scanner	●	-	●	●	●	●	●	-	●
Email Scanner	●	-	●	●	●	●	-	-	-
Different Update profiles	-	-	-	●	-	-	-	-	●
Own roaming update profile	-	-	-	●	-	●	-	●	-
Central Managed updates	-	●	-	●	-	●	●	●	●
Scan inside archives	-	-	●	●	●	●	●	-	-
Prevent access to harmful web sites (malware and phishing sites)	-	-	-	●	-	-	●	●	●
Scheduled Scan	●	●	-	-	●	●	●	-	●
Software Features									
PC Management Software	-	-	-	-	-	-	-	●	-
Central Management Software	-	-	-	●	-	●	-	●	-
Encryption with the Software	-	-	-	-	-	●	-	-	-
Synchronising	-	-	-	-	●	●	-	-	-
Windows 7 ready	-	-	-	-	-	●	●	●	-
Anti-Theft Features									
Report thief's location at SIM change	●	-	-	-	-	-	●	●	-
Report thief's phone number by SMS	●	-	●	●	-	●	●	-	-
Possibility to receive calls while locked	-	-	-	●	●	-	●	●	-
Possibility to make emergency calls while locked	-	-	-	●	●	-	●	●	●
Support									
Email Support	●	●	●	●	●	●	●	●	●
Online Help	●	●	●	●	●	●	●	●	●
Online Help (special URL designed for browsing with the phone)	●	-	●	●	●	-	●	●	●
User manual	●	●	●	●	●	●	●	●	●
User Forum	-	●	●	●	●	●	-	●	●
Online Chat	-	●	-	-	●	-	●	●	●
Support over Telephone	●	-	●	●	●	-	-	●	●
Supported languages (of support)	English	English, Danish, German, French, Spanish, Swedish, Norwegian	all	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish	English	all	English	all	English, Japanese
Price (depends from channels etc.)							-		
Price 1 phone / 1 year (EUR)	23	25	15	30	15	25	15	20	10
Price 3 phones / 2 years (EUR)	135	150	45	50	90	150	90	90	60
Various							-		
Direct Install on Device throug downloadlink	●	●	●	●	●	●	●	●	-
PC Application Install	-	-	-	-	-	●	●	●	-
Updates thru PC	●	-	-	-	-	-	-	-	-
Offline activation	-	-	-	●	-	-	-	-	-
No SIM activation	●	-	●	●	-	-	●	-	●
Updates (Auto/ On-Demand)	●	●	●	●	●	●	●	●	●
Quarantine	●	-	●	-	-	-	-	-	●
Blocking roaming data	-	-	-	●	●	●	-	-	-
SIM Matching	●	●	●	●	-	●	●	-	-
Statistics	●	-	●	●	●	●	●	●	●
Password protection of uninstallation	-	-	●	●	-	-	●	●	-
Backup							-		
Backup (online / memory card)	-	-	-	●	●	-	-	-	-
Backup of contacts	-	●	-	●	●	-	●	-	-
Backup of SMS/MMS	-	-	-	●	●	-	●	-	-
Backup of user data	-	-	-	●	●	-	●	-	-
Backup of configuration	-	-	-	-	●	-	-	-	-

	Windows Mobile						
	Blackbelt	Bullguard	ESET	F-Secure	Kaspersky	McAfee	Trend Micro
Product name:	UMU Mobile Security	BullGuard Mobile Security	ESET Mobile Security	F-Secure Mobile Security	Kaspersky Mobile Security	McAfee Mobile Security	Trend Micro Mobile Security
Supported OS versions:	5.0 and above	6.0, 6.1 and 6.5	5.0, 6.0, 6.1 and 6.5	6.0, 6.1 and 6.5	5.0 and above	6.0, 6.1 and 6.5	5.0, 6.0, 6.1 and 6.5
Supported Program languages:	English, French, Spanish, Traditional Chinese, Vietnamese	English	English, Czech, German, Spanish , French, Polish, Slovak, Turkish, Chinese Simplified, Chinese Traditional, Russian	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	English, Russian, German, French, Spanish, Italian, Dutch, Danish, Norwegian, Finnish, Swedish, Portugese, Brazilian Portugese, Polish, Turkish	English, Chinese Simplified, Chinese Traditional, German, French, Italian, Japanese, Dutch, Spanish, Portuguese, Brazilian Portuguese, Bahasa Indonesia, Korean, Swedish, French (Canadian), Spanish (Mexican), Russian, Norwegian, Danish, Finnish, Greek	English, German, Spanish, French, Russian, Traditional Chinese, Dutch
Locking Features:							
Lock Contacts	●	-	-	●	●	●	-
Lock Images/Files	●	-	-	●	●	●	-
Lock SMS/MMS	●	-	-	●	●	●	-
Lock SIM	●	-	-	-	-	●	-
Anti Spam Features							
Whitelist/Blacklist calls	-	●	●	-	●	-	-
Whitelist/Blacklist SMS	●	●	●	-	●	-	●
Whitelist/Blacklist MMS	-	-	●	-	-	-	●
Block known SMS/MMS spam	-	-	-	-	-	-	●
mark as spam with one klick	●	-	-	-	●	-	-
White- and Blacklisting with wildcards	●	-	-	-	●	-	-
Parental Control							
Pay Number locking	-	-	●	-	●	-	-
SMS Find (Localization of the Smartphone)	-	-	-	●	●	●	-
Log visited URLs	-	-	-	-	-	-	●
Firewall Features:							
Real-Time protection of inbound/outbound Traffic	-	●	●	●	●	-	●
Learning features	-	-	●	-	-	-	-
Different protection level	-	●	●	●	●	-	●
Different rule sets	-	●	-	●	-	-	●
Bluetooth protection (Spam etc.)	-	-	-	●	●	-	-
WiFi protection	-	-	-	●	●	-	-
Activity log	-	●	●	-	-	-	●
Protection log	-	●	●	-	●	-	●
Customizable firewall rules	-	●	●	●	-	-	●
Stateful packet inspection (conditional rules)	-	-	●	●	-	-	●
Remote Features							
Remote wipe of a stolen Smartphone	●	●	●	●	●	●	●
Remote GPS localization	-	●	-	●	●	●	-
SIM Watch (changing the SIM)	●	●	●	●	●	●	●
Remote installation of the Security System	-	-	●	-	●	-	-
Remote configuration	-	●	●	●	●	●	●
Remote updates	-	-	●	●	●	●	●
Central Management	-	●	●	●	●	●	●
Remote encryption	-	-	-	-	●	-	●
Central encryption policies	-	-	-	-	●	-	●
Encryption Features							
File System encryption	-	-	-	-	●	-	●
Password protected encryption	-	-	-	-	●	-	●
Encryption by data types (Outlook, Word, Excel, PDF, etc)	-	-	-	-	-	-	●
Admin decrypting option without password	-	-	-	-	-	-	●
Encryption by data location: on device, attached Memory Card	-	-	-	-	●	-	●
Authentication							
Policy controlled authentication	-	-	-	-	-	-	●
Access control	-	-	-	●	-	●	●
Encryption control	-	-	-	-	-	-	●
Port control: USB, Memory Cards, Bluetooth, WiFi	-	-	-	●	-	-	●
Resource Access control: IR, Camera, voice recording	-	-	-	-	-	-	●
Password policy: Strength, length, etc.	-	-	-	●	●	●	●
Maximum number of failed attempts	-	-	-	●	-	-	●
Grace period	-	-	-	●	-	-	-
Lock Screen with Password protection	●	●	-	●	●	●	●
AV Features							
Real Time File protection	●	●	●	●	●	●	●
On Demand Scan	●	●	●	●	●	●	●
Network protection	●	-	●	●	●	-	●
SMS/MMS Scanner	●	-	●	●	●	-	●
Email Scanner	●	-	●	●	●	●	-
Different Update profiles	-	-	●	●	-	-	●
Own roaming update profile	-	-	●	●	●	-	●
Central Managed updates	-	●	●	●	●	●	●
Scan inside archives	-	●	●	●	●	●	●
Prevent access to harmful web sites (malware and phishing sites)	-	-	-	●	-	●	●
Scheduled Scan	●	●	-	-	●	●	●
Software Features							
PC Management Software	-	-	-	-	-	-	●
Central Management Software	-	-	●	●	●	-	●
Encryption with the Software	-	-	-	-	●	-	●
Synchronising	-	-	●	-	●	-	-
Windows 7 ready	-	-	●	-	●	●	●
Anti-Theft Features							
Report thief's location at SIM change	●	-	-	-	-	●	●
Report thief's phone number by SMS	●	-	●	●	●	●	●
Possibility to receive calls while locked	-	-	-	●	-	●	●
Possibility to make emergency calls while locked	-	-	-	●	-	●	●
Support							
Email Support	●	●	●	●	●	●	●
Online Help	●	●	●	●	●	●	●
Online Help (special URL designed for browsing with the phone)	-	-	●	●	-	●	●
User manual	●	●	●	●	●	●	●
User Forum	-	●	●	●	●	-	●
Online Chat	-	●	-	-	-	●	●
Support over Telephone	●	-	●	-	-	-	●
Supported languages (of support)	English	English, Danish, German, French, Spanish, Swedish, Norwegian	all	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish	all	English	all
Price (depends from channels etc.)							
Price 1 phone / 1 year (EUR)	3,4	25	15	30	25	15	20
Price 3 phones / 2 years (EUR)	20	150	45	50	150	90	90
Various							
Direct Install on Device throug downloadlink	●	●	●	●	●	●	●
PC Application Install	●	●	-	-	●	●	●
Updates thru PC	●	-	-	●	-	-	●
Offline activation	-	-	-	●	-	-	●
No SIM activation	●	-	●	●	-	-	●
Updates (Auto/ On-Demand)	●	●	●	●	●	●	●
Quarantine	●	●	●	●	-	●	●
Blocking roaming data	-	-	●	●	●	-	-
SIM Matching	●	●	●	●	●	●	●
Statistics	●	-	●	●	●	●	●
Password protection of uninstallation	●	●	-	●	●	●	●
Backup							
Backup of contacts	-	●	-	-	-	●	-
Backup of SMS/MMS	-	-	-	-	-	●	-
Backup of user data	-	-	-	-	-	●	-

	Symbian						
	Blackbelt	Bullguard	ESET	F-Secure	Kaspersky	McAfee	Trend Micro
Product name:	BlackBelt Security	BullGuard Mobile Security	ESET Mobile Security	F-Secure Mobile Security	Kaspersky Mobile Security	McAfee Mobile Security	Trend Micro Mobile Security
Supported OS versions:	S60 2nd Edition, 3rd Edition, 5th Edition, Symbian^1, Symbian^2, Symbian^3 and above	Nokia devices - S60 3rd and 5th Edition	Symbian S60 3rd Edition Feature Pack 1 or 2 (Nokia only) Symbian S60 5th Edition (Nokia only) Symbian 3 (Nokia only)	S60 2nd Edition(Symbian 7.x / 8.x), S60 3rd Edition & 5th Edition (Symbian 9.x), Symbian^3	Symbian^3 or Series 60 9.1 - 9.4	Symbian S60 3rd/5th; Symbian^3	Symbian S60 3rd/5th; Symbian^3
Supported Program languages:	English, French, Spanish, Traditional Chinese, Vietnamese	English	English, Czech, German, Spanish , French, Polish, Slovak, Turkish, Chinese Simplified, Chinese Traditional, Russian	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	English, Russian, German, French, Spanish, Italian, Dutch, Danish, Norwegian, Finnish, Swedish, Portugese, Brazilian Portugese, Polish, Turkish	English, Chinese Simplified, Chinese Traditional, German, French, Italian, Japanese, Dutch, Spanish, Portuguese, Brazilian Portuguese, Bahasa Indonesia, Korean, Swedish, French (Canadian), Spanish (Mexican), Russian, Norwegian, Danish, Finnish, Greek	English, German, Spanish, French, Russian, Traditional Chinese, Dutch
Locking Features:							
Lock Contacts	●	-	-	●	●	●	-
Lock Images/Files	●	-	-	●	●	●	-
Lock SMS/MMS	●	-	-	●	●	●	-
Lock SIM	●	-	-	-	-	●	-
Anti Spam Features							
Whitelist/Blacklist calls	-	●	●	-	●	-	-
Whitelist/Blacklist SMS	●	●	●	-	●	-	●
Whitelist/Blacklist MMS	-	-	●	-	-	-	●
Block known SMS/MMS spam	-	-	-	-	-	-	●
mark as spam with one klick	●	-	-	-	●	-	-
White- and Blacklisting with wildcards	●	-	-	-	●	-	-
Block attachments/applications/file extensions	-	-	-	-	-	●	-
Parental Control							
Pay Number locking	-	-	●	-	●	-	-
SMS Find (Localization of the Smartphone)	-	-	-	●	●	●	-
Log visited URLs	-	-	-	-	-	-	●
Firewall Features:							
Real-Time protection of inbound/outbound Traffic	-	●	●	●	●	-	●
Learning features	-	-	●	-	-	-	-
Different protection level	-	●	●	●	●	-	●
Different rule sets	-	●	-	●	-	-	●
Bluetooth protection (Spam etc.)	-	-	-	●	●	-	-
WiFi protection	-	-	-	●	●	-	-
Activity log	-	●	●	-	-	-	●
Protection log	-	●	●	-	●	-	●
Customizable firewall rules	-	●	●	●	-	-	●
Stateful packet inspection (conditional rules)	-	-	●	●	-	-	●
Remote Features							
Remote wipe of a stolen Smartphone	●	●	●	●	●	●	●
Remote GPS localization	-	●	-	●	●	●	-
SIM Watch (changing the SIM)	●	●	●	●	●	●	●
Remote installation of the Security System	-	-	●	-	●	-	-
Remote configuration	-	●	●	●	●	●	●
Remote updates	-	-	●	●	●	●	●
Central Management	-	●	●	●	●	●	●
Remote encryption	-	-	-	-	●	-	●
Central encryption policies	-	-	-	-	●	-	●
Encryption Features							
File System encryption	-	-	-	-	●	-	●
Password protected encryption	-	-	-	-	●	-	●
Encryption by data types (Outlook, Word, Excel, PDF, etc)	-	-	-	-	-	-	●
Admin decrypting option without password	-	-	-	-	-	-	●
Encryption by data location: on device, attached Memory Card	-	-	-	-	●	-	●
Authentication							
Policy controlled authentication	-	-	-	-	-	-	●
Access control	-	-	-	●	-	●	●
Encryption control	-	-	-	-	-	-	●
Port control: USB, Memory Cards, Bluetooth, WiFi	-	-	-	●	-	-	-
Password policy: Strength, length, etc.	-	-	-	●	●	●	●
Maximum number of failed attempts	-	-	-	●	-	-	●
Grace period	-	-	-	●	-	-	-
Lock Screen with Password protection	●	●	-	●	●	●	●
AV Features							
Real Time File protection	●	●	●	●	●	●	●
On Demand Scan	●	●	●	●	●	●	●
Network protection	●	-	●	●	●	-	
SMS/MMS Scanner	●	-	●	●	●	●	●
Email Scanner	●	-	●	●	●	●	-
Different Update profiles	-	-	●	●	-	-	●
Own roaming update profile	-	-	●	●	●	-	●
Central Managed updates	-	●	●	●	●	●	●
Scan inside archives	-	●	●	●	●	●	●
Prevent access to harmful web sites (malware and phishing sites)	-	-	-	●	-	●	●
Scheduled Scan	●	●	-	-	●	●	●
Software Features							
PC Management Software	-	-	-	-	-	-	●
Central Management Software	-	-	●	●	●	-	●
Encryption with the Software	-	-	-	-	●	-	●
Synchronising	-	-	●	-	●	-	-
Windows 7 ready	-	-	●	-	●	●	●
Anti-Theft Features							
Report thief's location at SIM change	●	-	-	-	-	●	●
Report thief's phone number by SMS	●	-	●	●	●	●	●
Possibility to receive calls while locked	-	-	-	●	-	●	●
Possibility to make emergency calls while locked	-	-	-	●	-	●	●
Support							
Email Support	●	●	●	●	●	●	●
Online Help	●	●	●	●	●	●	●
Online Help (special URL designed for browsing with the phone)	-	-	●	●	-	●	●
User manual	●	●	●	●	●	●	●
User Forum	-	●	●	●	●	-	●
Online Chat	-	●	-	-	-	●	●
Support over Telephone	●	-	●	●	-	-	●
Supported languages (of support)	English	English, Danish, German, French, Spanish, Swedish, Norwegian	all	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish	all	English	all
Price (depends from channels etc.)							
Price 1 phone / 1 year (EUR)	23	25	15	30	25	15	10
Price 3 phones / 2 years (EUR)	136	150	45	100	150	90	60
Various							
Direct Install on Device throug downloadlink	●		●	●	●	●	●
PC Application Install	●	-	-	-	●	●	●
Updates thru PC	●	-	-	●	-	-	●
Offline activation	-	-	-	●	-	-	●
No SIM activation	●	-	●	●	-	-	●
Updates (Auto/ On-Demand)	●	●	●	●	●	●	●
Quarantine	●	●	●	●	-	●	●
Blocking roaming data	-	-	●	●	●	-	-
SIM Matching	●	●	●	●	●	●	●
Statistics	●	-	●	●	●	●	●
PW protection of uninstallation	●	-	-	●	●	●	●
Backup							
Backup (online / memory card)	-	-	-	●	-	-	-
Backup of contacts	-	●	-	●	-	●	-
Backup of SMS/MMS	-	-	-	●	-	●	-
Backup of user data	-	-	-	●	-	●	-

iPhone	
	F-Secure
Product name:	***depends on operator***
Supported OS versions:	iOS 4
Supported Program languages:	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish
Software Features	
Central Management Software	●
Support	
Email Support	●
Online Help	●
Online Help (special URL designed for browsing with the phone)	●
User manual	●
User Forum	●
Support over Telephone	●
Supported languages (of support)	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish
Price (depends from channels etc.)	
Price 1 phone / 1 year (USD/EUR)	Price depends on channel
Price 3 phones / 2 years (USD/EUR)	Price depends on channel
Various	
Direct Install on Device throug downloadlink	●
Offline activation	●
No SIM activation	●
Updates (Auto/ On-Demand)	●
Blocking roaming data	●
Statistics	●
Backup	
Backup (online / memory card)	●
Backup of contacts	●
Backup of SMS/MMS	●
Backup of user data	●

Blackberry				
	Bullguard	**F-Secure**	**Kaspersky**	**McAfee**
Product name:	**BullGuard Mobile Security**	**F-Secure Mobile Security**	**Kaspersky Mobile Security**	**McAfee Mobile Security**
Supported OS versions:	4.2 and higher	6.0	4.5 and higher	4.5 and higher
Supported Program languages:	English	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	English, Russian, German, French, Spanish, Italian, Dutch, Danish, Norwegian, Finnish, Swedish, Portugese, Brazilian Portugese, Polish, Turkish	English, Chinese Simplified, Chinese Traditional, German, French, Italian, Japanese, Dutch, Spanish, Portuguese, Brazilian Portuguese, Bahasa Indonesia, Korean, Swedish, French (Canadian), Spanish (Mexican), Russian, Norwegian, Danish, Finnish, Greek
Locking Features:				
Lock Contacts	-	●	●	●
Lock Images/Files	-	●	●	●
Lock SMS/MMS	-	●	●	●
Lock SIM	-	-	-	●
Anti Spam Features				
Whitelist/Blacklist calls	-	-	●	-
Whitelist/Blacklist SMS	-	-	●	-
mark as spam with one klick	-	-	●	-
White- and Blacklisting with wildcards	-	-	●	-
Block attachments/applications/file extensions	-	-	-	●
Parental Control				
SMS Find (Localization of the Smartphone)	-	●	●	●
Remote Features	-			
Remote wipe of a stolen Smartphone	●	●	●	●
Remote GPS localization	●	●	●	●
SIM Watch (changing the SIM)	●	●	●	●
Remote installation of the Security System	-	-	●	-
Remote configuration	●	●	●	●
Remote updates	-	●	●	●
Central Management	●	●	●	●
Authentication				
Access control	-	●	-	●
Password policy: Strength, length, etc.	-	●	●	●
Lock Screen with Password protection	●	●	●	●
AV Features				
Real Time File protection	●	-	-	●
On Demand Scan	●	-	-	●
Email Scanner	-	-	-	●
Own roaming update profile	-	●	-	-
Central Managed updates	●	●	-	●
Scan inside archives	-	-	-	●
Prevent access to harmful web sites (malware and phishing sites)	-	-	-	●
Scheduled Scan	-	-	-	●
Software Features				
Central Management Software	-	●	●	-
Synchronising	-	-	●	-
Windows 7 ready	-	-	●	●
Anti-Theft Features				
Report thief's location at SIM change	-	-	-	●
Report thief's phone number by SMS	-	●	●	●
Possibility to receive calls while locked	-	●	-	●
Possibility to make emergency calls while locked	-	●	-	●
Support				
Email Support	●	●	●	●
Online Help	●	●	●	●
Online Help (special URL designed for browsing with the phone)	-	●	-	●
User manual	●	●	●	●
User Forum	●	●	●	-
Online Chat	●	-	-	●
Support over Telephone	-	●	-	-
Supported languages (of support)	English, Danish, German, French, Spanish, Swedish, Norwegian	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish	all	English
Price (depends from channels etc.)				
Price 1 phone / 1 year (USD/EUR)	25	30	25	15
Price 3 phones / 2 years (USD/EUR)	150	150	150	90
Various				
Direct Install on Device throug downloadlink	●	●	●	●
PC Application Install	-	-	●	●
Offline activation	-	●	-	-
No SIM activation	-	●	-	-
Updates (Auto/ On-Demand)	●	●	●	●
Quarantine	●	-	-	-
Blocking roaming data	-	-	●	-
SIM Matching	●	●	●	●
Statistics	-	●	●	●
PW protection of uninstallation	-	●	●	●
Backup				
Backup (online / memory card)	-	●	-	-
Backup of contacts	●	●	-	●
Backup of SMS/MMS	-	●	-	●
Backup of user data	-	●	-	●

Android Free			
	F-Secure	Trend Micro	Webroot
Product name:	F-Secure Mobile Security	Trend Micro Mobile Security Personal Edition	Webroot Mobile Security
Supported OS versions:	1.6 - 2.3, 3.x	2.2 and above	2.1 and above
Supported Program languages:	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	English, Japanese, German, French, Italian, Spanish, Russian, Dutch, Brazil-Portuguese, Simplified Chinese, Traditional Chinese, Korean.	English, Japanese
Locking Features:			
Lock Contacts	●	-	●
Lock Images/Files	●	-	●
Lock SMS/MMS	●	-	●
Anti Spam Features			
Whitelist/Blacklist calls	-	-	●
Whitelist/Blacklist SMS	-	-	●
Whitelist/Blacklist MMS	-	-	●
Block known SMS/MMS spam	-	-	●
Parental Control			
SMS Find (Localization of the Smartphone)	-	-	●
Remote Features			
Remote wipe of a stolen Smartphone	●	-	-
Remote GPS localization	●	-	●
SIM Watch (changing the SIM)	●	-	-
Remote configuration	●	-	●
Remote updates	●	-	●
Central Management	●	-	●
AV Features			
Real Time File protection	-	●	●
On Demand Scan	-	●	●
Network protection	-	-	●
SMS/MMS Scanner	-	-	●
Different Update profiles	-	-	●
Own roaming update profile	-	●	-
Central Managed updates	-	-	●
Prevent access to harmful web sites (malware and phishing sites)	-	-	●
Scheduled Scan	-	-	●
Anti-Theft Features			
Report thief's phone number by SMS	●	-	-
Possibility to receive calls while locked	●	-	-
Possibility to make emergency calls while locked	●	-	●
Support			
Email Support	●	-	●
Online Help	●	●	●
Online Help (special URL designed for browsing with the phone)	●	●	●
User manual	●	●	●
User Forum	●	-	●
Online Chat	-	-	●
Support over Telephone	●	-	-
Supported languages (of support)	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish	English, Japanese	English, Japanese
Various			
Direct Install on Device throug downloadlink	●	-	-
No SIM activation	-	-	●
Updates (Auto/ On-Demand)	●	●	●
Quarantine	-	●	●
SIM Matching	●	-	-
Statistics	●	●	●

Windows Mobile Free	
	F-Secure
Product name:	***F-Secure Mobile Security***
Supported OS versions:	6.0, 6.1 and 6.5
Supported Program languages:	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish
Locking Features:	
Lock Contacts	●
Lock Images/Files	●
Lock SMS/MMS	●
Remote Features	
Remote wipe of a stolen Smartphone	●
Remote GPS localization	●
SIM Watch (changing the SIM)	●
Remote configuration	●
Remote updates	●
Central Management	●
Anti-Theft Features	
Report thief's phone number by SMS	●
Possibility to receive calls while locked	●
Possibility to make emergency calls while locked	●
Support	
Email Support	●
Online Help	●
Online Help (special URL designed for browsing with the phone)	●
User manual	●
User Forum	●
Support over Telephone	●
Supported languages (of support)	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish
Various	
Direct Install on Device throug downloadlink	●
Updates (Auto/ On-Demand)	●
SIM Matching	●
Statistics	●
PW protection of uninstallation	●

Symbian Free	
	F-Secure
Product name:	***F-Secure Mobile Security***
Supported OS versions:	S60 2nd Edition(Symbian 7.x / 8.x), S60 3rd Edition & 5th Edition (Symbian 9.x), Symbian^3
Supported Program languages:	English, Arabic, Bulgarian, Simplified Chinese, Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesia, Italian, Japanese, Korean, Malay, Norwegian, Polish, Brazilian Portuguese, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish
Locking Features:	
Lock Contacts	●
Lock Images/Files	●
Lock SMS/MMS	●
Remote Features	
Remote wipe of a stolen Smartphone	●
Remote GPS localization	●
SIM Watch (changing the SIM)	●
Remote configuration	●
Remote updates	●
Central Management	●
Anti-Theft Features	
Report thief's phone number by SMS	●
Possibility to receive calls while locked	●
Possibility to make emergency calls while locked	●
Support	
Email Support	●
Online Help	●
Online Help (special URL designed for browsing with the phone)	●
User manual	●
User Forum	●
Support over Telephone	●
Supported languages (of support)	English, Finnish, French, Dutch, Danish, German, Chienese, Italian, Norway, Polish, Swedish
Various	
Direct Install on Device throug downloadlink	●
Updates (Auto/ On-Demand)	●
SIM Matching	●
Statistics	●
PW protection of uninstallation	●

iPhone Free	
	Trend Micro
Product name:	***Smart Surfing for iOS***
Supported OS versions:	iOS 3.1 and above
Supported Program languages:	English, Japanese
Parental Control	
Log visited URLs	●
AV Features	
Prevent access to harmful web sites (malware and phishing sites)	●
Support	
Email Support	●
Online Help	●
Online Help (special URL designed for browsing with the phone)	●
Online Chat	●
Supported languages (of support)	all
Various	
Direct Install on Device throug downloadlink	●
PC Application Install	●
Offline activation	●

Copyright and Disclaimer

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

AV-Comparatives e.V. (September 2011)