Product Review

Mobile Security

Sprache: Deutsch
August 2010
Letzte Überarbeitung: 5. September 2010

www.av-comparatives.org

Inhaltsverzeichnis

Allgemein 3

ESET Mobile Security 1.3 4

F-Secure Mobile Security 6.1 6

Kaspersky Mobile Security 9 9

Trend Micro Mobile Security 6.5 13

Fazit 16

Feature Liste Mobile Security 17

Allgemein

Smartphones erfreuen sich in den heutigen Tagen an immer mehr Beliebtheit. Durch die Integrierung von neuen Technologien, an deren Verwendung früher nur am heimischen PC zu denken war, entwickeln sich Smartphones zu wahren Kraftprotzen. Dies bringt jedoch auch einige Risiken mit sich. Seitdem Smartphones immer häufiger eingesetzt werden um im Internet zu surfen, Daten zu übertragen und auch als Datenzentrale in Unternehmen herangezogen werden, steigt das Risiko. Nicht nur dass sich Malware auf dem Mobiltelefon einnisten kann, viel problematischer sind Attacken auf Daten oder Phishing-Angriffe. In Zeiten von Beetaggs, QR oder Datamatrix ist ein Phishing-Angriff leicht zu starten.

Fast jeder verwendet zu Hause auf seinem PC ein Security-Produkt. Jedoch ist der Einsatz auf Mobiltelefonen nicht weit verbreitet. Und das obwohl oft wichtige persönliche Daten, private Fotos und manchmal Firmendaten darauf gespeichert werden.

Dadurch, dass Smartphones sehr teuer und klein sind, sind sie auch einem weiteren Risiko ausgesetzt: Sie sind ein begehrtes Ziel für Diebe. Es muss Dieben schwer gemacht werden, auf wichtige Daten zuzugreifen! Der Anreiz eines Diebstahles muss wegfallen. Ohne mobile Sicherheit haben Kriminelle leichtes Spiel. Die Diebe entwenden das Telefon, tauschen die SIM-Karte aus, und das Telefon ist nicht mehr erreichbar. Oder sie telefonieren auf Kosten des Geprellten oder verwenden es gar für weitere kriminelle Zwecke.

Um diesem Szenario entgegenzuwirken verfügen heutige Sicherheitsprodukte für Mobilgeräte über verschiedene Sicherheitsfeatures.

Diebstahlsicherung

Ein sehr nützliches Feature ist die Diebstahlsicherung des Smartphones. Dabei hat der User nach einem Diebstahl oder Verlust die Möglichkeit, das Telefon zu sperren, zu löschen und auch zu orten. Dazu muss der User eine SMS mit einem beliebigen Mobiltelefon an sein Smartphone mit dem jeweiligen Code und Passwort senden. Anschließend erhält der User eine SMS mit den GPS Daten des Smartphones.

Dieses Feature ist sehr nützlich, kann jedoch auch missbräuchlich zur Ortung von Personen verwendet werden. Es besteht die Möglichkeit, dass eine Person ein Security-Produkt auf dem Smartphone einer anderen Person installiert oder jemanden ein Mobiltelefon mit integriertem Security-Produkt mit Ortung schenkt.

Firewall

Ähnlich den Einstellungen der Firewall am heimischen PC hat der User auch hier die Möglichkeit Regeln zu definieren, welchen es Anwendungen erlaubt, Verbindungen aufzubauen und entgegenzunehmen oder eben nicht.

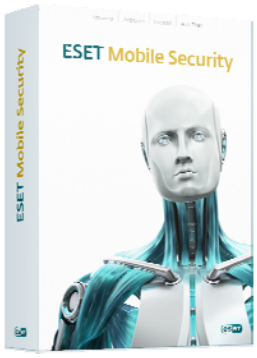
Virenschutz

Mit Hilfe des Malwareschutzes werden Smartphones auf Schadsoftware durchsucht und diese entsprechend gelöscht oder in Quarantäne verschoben. Um dieses Feature effizient nutzen zu können, muss der Virenschutz mit Updates auf dem neuesten Stand gehalten werden. Aufpassen muss man im Ausland, dass man nicht in die Roamingfalle tappt.

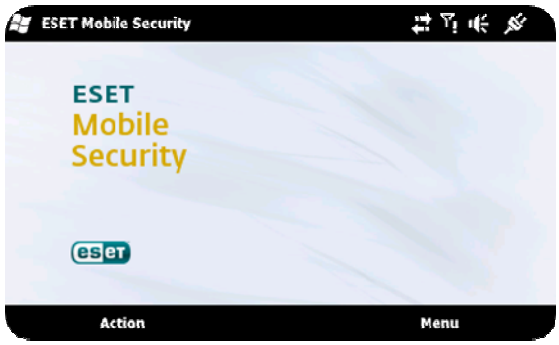
Getestet wurde unter Windows Mobile und Symbian. Welche anderen Plattformen die Produkte der jeweiligen Hersteller unterstützen, kann der Featureliste entnommen werden.

In unserem Report finden Sie Details zu den Produkten der führenden Anbieter.

ESET Mobile Security



ESET bietet in seinem Sortiment nun auch eine mobile Sicherheitssuite namens ESET Mobile Security für Smartphones und Pocket-PCs an. Moderne Sicherheitsfeatures wie Diebstahlsicherung und Firewall sind integriert. Das User Interface ist sehr einfach und übersichtlich gestaltet.



Installation

Die Installation von ESET Mobile Security ging schnell und problemlos über das Telefon von statten (nur 0.5 MB werden geladen). Nach der Installation musste das Produkt manuell aktiviert werden.

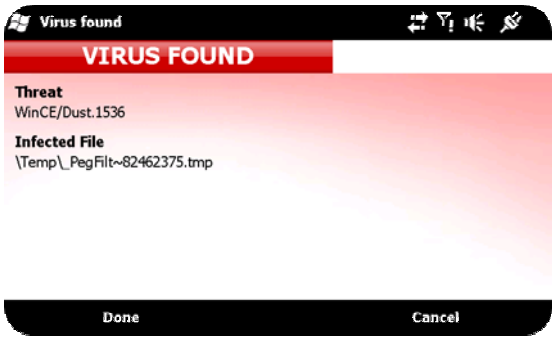
Starten des Programms

ESET Mobile Security kann direkt über den Desktop des Smartphones gestartet werden. Eine Passworteingabe ist nicht erforderlich. Der User hat die Möglichkeit ein Passwort manuell zu vergeben, welches zum Beispiel bei Änderungen in der Diebstahlsicherung eingegeben werden muss.

Echtzeitschutz

Ist der Echtzeitschutz aktiviert, fungiert ESET Mobile Security als Hintergrundwächter, d.h. das Dateien in Echtzeit auf Viren überprüft werden, welche ausgeführt, geöffnet oder gespeichert werden. Standardmäßig ist der Echtzeitschutz aktiviert wobei keinerlei Performance-Einbuße spürbar war.

Um den Echtzeitschutz zu testen wurde versucht einen Virus auf das Smartphone zu laden. ESET Mobile Security hat diesen sofort erfolgreich blockiert und folgende Meldung dargestellt.



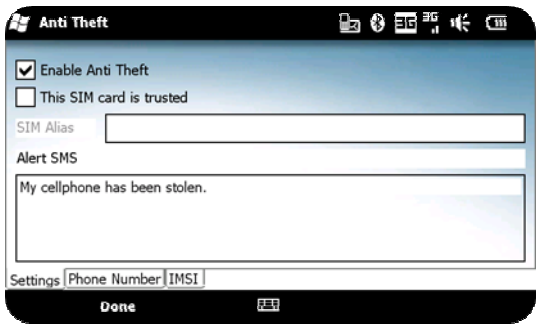
Spam-Filter

Der Spam-Filter erlaubt es dem User, seinen SMS und MMS Verkehr zu filtern und zu reduzieren. Mit Hilfe von Listen (Negativ-, Positivliste), kann der User Telefonnummern hinzufügen, welche geblockt bzw. zugelassen werden.

Diebstahlsicherung

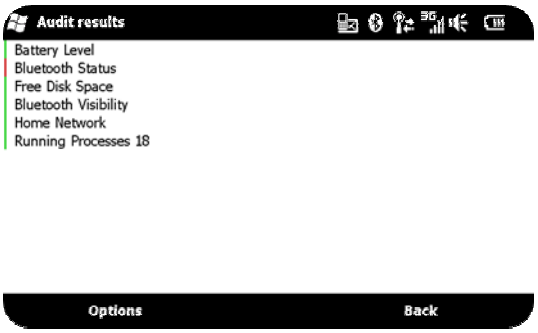
Auch ESET integriert das Konzept der Diebstahlsicherung. Diese ermöglicht ein ferngesteuertes Löschen des Smartphones sowie das Senden einer SMS bei einem SIM-Kartentausch. Positiv aufgefallen ist, dass ESET die Diebstahlsicherung standardmäßig aktiviert und die Möglichkeit besteht, eine vertrauenswürdige SIM-Karte hinzuzufügen, welche bei der

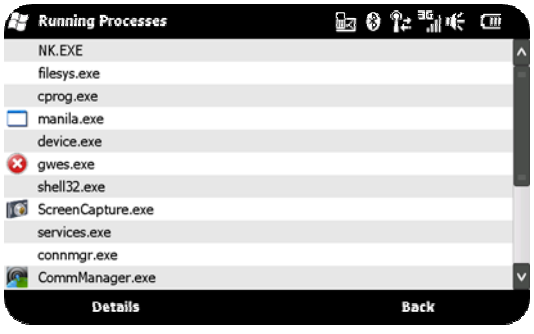
Benachrichtigung eines SIM-Kartentausch ausgenommen wird.



Sicherheitsprüfung

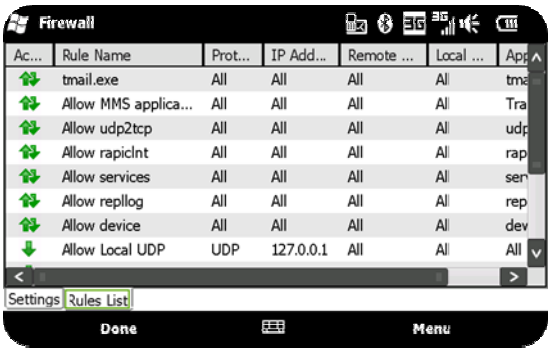
ESET Mobile Security integriert ein Verfahren zur Sicherheitsprüfung, welches Komponenten wie Batteriestatus, Bluetooth-Status und laufende Prozesse überwacht. Nach einer Prüfung wird der Status der einzelnen Komponenten farblich dargestellt und mit einem definierbaren Grenzwert verglichen. Befindet sich der Wert einer Komponente unterhalb des Grenzwertes, wird diese rot markiert und dem Anwender ermöglicht diese zu korrigieren.





Firewall

Ähnlich zu anderen Herstellern, bietet ESET Mobile Security die Möglichkeit an, den gesamten Netzwerkverkehr zu blockieren, zu erlauben bzw. benutzerdefinierte Einstellungen vorzunehmen.



Deinstallation

Die Deinstallation ist problemlos über die Windows Mobile „Programme entfernen“ Routine möglich. Um ein unbefugtes Löschen zu vermeiden, muss das Passwort von ESET Mobile Security eingegeben werden.

Fazit

ESET Mobile Security ist ein übersichtliches Sicherheits-Produkt, welches von jedem User sehr einfach bedient werden kann. Für Benutzer, die mehrere SIM-Karten verwenden und nicht auf einen Diebstahlschutz verzichten wollen, hat ESET eine elegante Lösung gefunden.

Preislich liegt ESET Mobile Security im unteren Bereich, jedoch muss man auf die Möglichkeit einer Ortung bzw. Verschlüsselung verzichten. ESET ist ein neues Produkt und wird möglicherweise in Zukunft weitere Sicherheitsfunktionen integrieren.

F-Secure Mobile Security

Die mobile Sicherheitssoftware von F-Secure präsentiert sich in einer übersichtlichen Optik. Auf unserem Testgerät, dem HTC Touch Pro2, waren die Schaltflächen groß genug gestalten, um sie über den Touch Screen auch mit den Fingern bedienen zu können. Die Benutzeroberfläche ist leicht verständlich gestaltet, was dem User ein lesen des Benutzerhandbuches ersparen kann. Positiv aufgefallen ist, das F-Secure Mobile Security über die derzeit aktuellsten Schutzmechanismen (Virenschutz, Firewall und Diebstahlsicherung) verfügt.

Installation

Für den Installationsvorgang hat der User zum Einen die Möglichkeit, die Software direkt über das Smartphone herunterzuladen, was bei einem nicht vorhandenen Internetpaket teuer werden kann (knapp 3 MB werden geladen), zum Anderen die Möglichkeit, die Software direkt auf den PC zu laden und anschließend mit ActiveSync zu installieren.

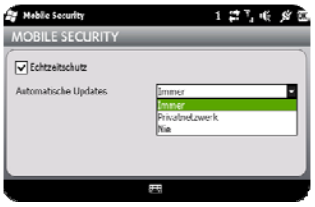
In unserem Test wurde die Software direkt über das Smartphone heruntergeladen und installiert. Der User ist nach der Installation sofort geschützt, um die Firewall zu starten muss das Mobiltelefon neu gestartet werden. Die Installation gestaltet sich denkbar einfach.

Starten des Programms

Nach einer erfolgreichen Installation kann das Programm direkt über eine Verknüpfung am Desktop gestartet werden. Eine Passworteingabe ist nicht vorhanden.

Virenschutz

Der Virenschutz wird nach der Installation standardmäßig aktiviert. Danach wird dem User aus Sicherheitsgründen empfohlen, eine erste Prüfung auf schädliche Software laufen zu lassen. Anschließend muss der User definieren, auf welche Art und Weise Updates bezogen werden sollen.



Dazu werden drei Möglichkeiten angeboten. Zum einen kann eingestellt werden, dass Updates immer bezogen werden. Hier ist eine Internet-Flatrate am Mobilgerät empfehlenswert.

Zum anderen kann konfiguriert werden, dass nur im Privatnetzwerk ein Update vollzogen wird, um Traffic bzw. Roamingkosten zu sparen. Zuletzt können Updates auch komplett deaktiviert werden.

In unserem Test haben wir zwei Viren auf das Smartphone geladen, welche sofort von

F-Secure Mobile Security entdeckt und in die Quarantäne verschoben wurden.

Um den Browser-Schutz zu testen, wurde im dem Windows Internet Explorer eine Phishing Seite geöffnet, welche als Bedrohung identifiziert wurde. Die folgende Meldung informiert den User bezüglich einer schädlichen Webseite.

Firewall

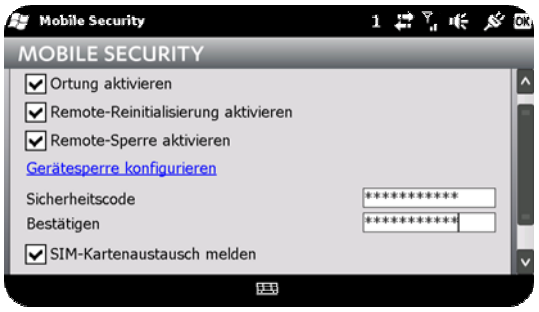
Nach einer erfolgreichen Installation wird die Sicherheitsstufe der Firewall auf „Normal" gesetzt. Die Sicherheitsstufe umfasst Regelsätze wie, „Alle ablehnen", „Hoch", „Alle zulassen" und „Benutzerdefiniert". In einem Regelsatz können verschiedenste Dienste, wie DNS, DHCP, SMTP, HTTP, usw. blockiert oder zugelassen werden.

Diebstahlsicherung

Die Diebstahlsicherung von F-Secure Mobile Security integriert vier nützliche Features auf Ihrem Smartphone.

Ortung aktivieren

Dieser Dienst ermöglicht eine Ortung des Mobiltelefons. Dabei kann der User mit jedem beliebigen SMS-fähigen Telefon eine Nachricht an sein verloren gegangenes Smartphone schicken. Die Nachricht muss ein spezielles Codewort gefolgt von einem Sicherheitscode, welchen der User im Vorhinein in den Einstellungen der Diebstahlsicherung definiert hat, beinhalten. Im Falle von F-Secure Mobile Security muss das Codewort #locate# gefolgt vom Sicherheitscode gesendet werden. Bei einer erfolgreichen Ortung erhält der User die GPS Daten seines verloren gegangenen Smartphones. Wenn kein GPS Signal empfangen werden kann, wie etwa in engen Häuserschluchten oder Gebäuden, weicht die Software auf Cell-ID Erkennung aus und liefert einen Näherungswert.



Remote-Reinitialisierung aktivieren

Mit Hilfe dieses Dienstes, kann der User sein Smartphone ferngesteuert löschen. Dabei werden alle Daten auf dem Mobiltelefon gelöscht. Dies geschieht wieder mit einer SMS mit dem Codewort #wipe# gefolgt vom Sicherheitscode.

Mit Hilfe der Remote-Sperre, hat der User die Möglichkeit sein Mobiltelefon ferngesteuert zu sperren. Um diesen Dienst nützen zu können muss eine Gerätesperre konfiguriert werden. Anschließend hat der User die Möglichkeit sein Telefon mit dem Codewort #lock# gefolgt vom Sicherheitscode zu sperren.

Nach einer Remote-Sperre können Notrufnummern angewählt werden, was bei einigen anderen Produkten nicht möglich war. Damit erfüllt F-Secure Mobile Security EU Richtlinien, welche besagen, dass Notrufe auf gesperrten Telefonen durchführbar sein müssen.

SIM-Kartentausch melden

Dieser Dienst soll verhindern, dass ein gestohlen oder verloren gegangenes Telefon nach einem SIM-Kartentausch nicht mehr gesperrt, gelöscht oder geortet werden kann. Sollte das Telefon jedoch mit einer neuen SIM-Karte ausgestattet werden, kann der User diese Dienste nicht mehr nutzen, da das Telefon nun über eine andere Telefonnummer erreichbar ist. Hat der User jedoch den „Dienst SIM-Kartentausch melden" aktiviert, wird an eine vorher definierte Telefonnummer eine SMS mit der Telefonnummer der neuen SIM Karte gesendet. Somit ist auch bei einem SIM-Kartentausch durch den Dieb eine Sperre möglich.

Ein kleines Manko von F-Secure Mobile Security ist jedoch, dass diese Dienste nicht standardmäßig aktiviert werden, bzw. das der User nicht hingewiesen wird, diese Dienste zu nützen, bevor es im Falle eines Diebstahles zu spät ist.

Ein weiteres sehr interessantes Feature der Diebstahlsicherung ist „SIM-Kartentausch melden". Hierbei wird einer vorher definierten Telefonnummer ein SMS-Alarm geschickt, welcher die Telefonnummer der neu installierten SIM Karte als SMS verschickt. Somit hat der User die Möglichkeit, auch nach einem SIM-Kartentausch, sein Telefon zu sperren, löschen und orten.

Deinstallation

Um F-Secure Mobile Security zu deinstallieren, wurde die „Programme entfernen" Routine von Windows Mobile verwendet. Nach ein paar Sekunden wurde die Software vom Smartphone problemlos gelöscht.

Ohne Gerätesperre wirkungslos

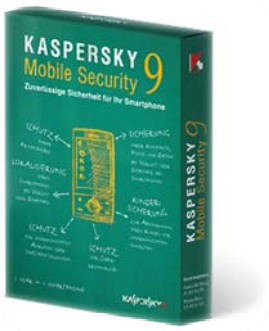
Hat man die gewünschten Schutzeinstellungen getroffen, ist man größtenteils geschützt. In unserem Test hatte man jedoch die Möglichkeit, den Sicherheitscode der Diebstahlsicherung von Windows Mobile zu ändern, ohne dass der alte Code eingegeben werden musste. Sogar alle Einstellungen von F-Secure Mobile Security konnten ohne eine Passworteingabe geändert werden, solange die Gerätesperre noch nicht aktiv war. Somit hätte ein Dieb die Möglichkeit, innerhalb von maximal 24 Stunden nach dem Diebstahl F-Secure Mobile Security zu deaktivieren, selbst wenn das Kommando „Sperren" geschickt wurde. Dies hängt aber auch von den Nutzereinstellungen ab. F-Secure hat versprochen, diese Lücke zu schließen und mit dem nächsten Release automatisch an alle Windows Mobile User auszuliefern. Eine einfache Passworteingabe, bevor die Einstellungen von F-Secure Mobile Security geändert werden könnten, würde schon genügen, um einem Dieb den Gerätezugriff zu erschweren.

Fazit

Mit F-Secure Mobile Security ist ihr Smartphone von Dieben und Malware geschützt. Das User-Interface ist übersichtlich gestaltet und leicht verständlich.

Der Preis ist im Vergleich zu anderen Produkten eher im höheren Segment angesetzt. 12 Monate Schutz pro Smartphone kosten knapp 40 Euro. Im OVI-Store haben wir es aber schon ab 10 Euro gesehen.

Kaspersky Mobile Security



Im Bereich mobiler Sicherheit bietet Kaspersky nun schon die 9te Version seiner Mobile Security Suite an. Diese besteht aus seiner Vielzahl von Anwendungen, welche als sehr ausgereift scheinen. Zu den Schutzmechanismen zählen Anti-Viren Schutz, Diebstahlschutz, Privatsphäre, Verschlüsselung, Anti-Spam, Kindersicherung sowie eine Firewall. Die Benutzeroberfläche ist sehr leicht verständlich und übersichtlich gestaltet. Einen großen Pluspunkt erhält das User-Interface durch sein Informationsmanagement. Will ein User zum Beispiel den SMS-Block aktivieren, erhält dieser sofort eine Meldung (Tooltip). Bei anderen Produkten war dies nicht der Fall. Über die Komponente Schutzstatus werden die Einstellungen von Kaspersky Mobile Security 9 in Form eines Überblickes dargestellt.

Installation

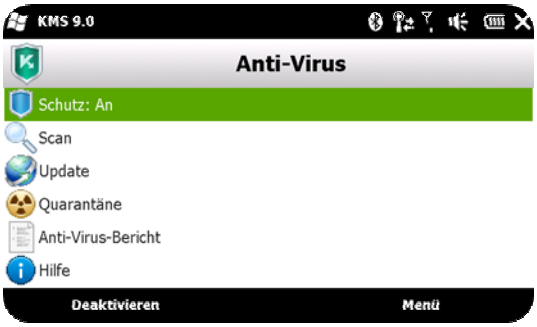
Die Installation von Kaspersky Mobile Security 9 über die mitgelieferte CD verlief problemlos. Der User wird gut durch die Installation geführt. Nach der Aktivierung musste der Sicherheitscode eingegeben werden, welcher beim Starten des Programms benötigt wird. Kaspersky bewertet diesen und informiert den User im Falle eines unsicheren Codes.

Starten des Programms

Nach einer erfolgreichen Installation kann das Programm über eine Verknüpfung am Desktop gestartet werden. Anschließend wird der User aufgefordert den Sicherheitscode einzugeben, welcher nach der Aktivierung festgelegt wurde.

Virenschutz

Der Virenschutz ist standardmäßig aktiviert, jedoch wurde nach der Installation kein automatischer Viren-Scan durchgeführt. Kaspersky verfügt über die Möglichkeit, einen Scan-Zeitplan einzurichten, dieser muss aber manuell eingestellt werden. Standardmäßig werden die Virendefinitionen nach einem einmal wöchentlichen Zeitplan heruntergeladen. Der Modus „Update im Roaming“ ist voreingestellt.



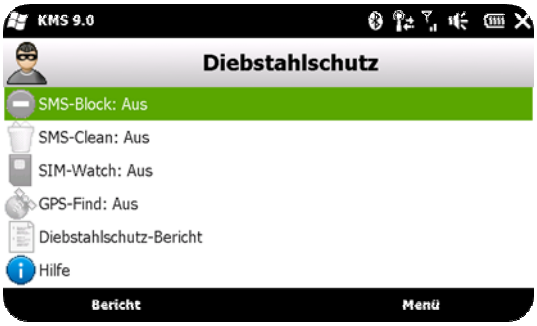
Bei unserem Versuch das Smartphone mit einem Virus zu infizieren, gab Kaspersky Mobile Security nur eine akustische Meldung von sich, um den User über eine Bedrohung zu informieren. Die Standardeinstellung bei Virenfund ist das verschieben in die Quarantäne. Alternativ kann das Objekt gelöscht oder der Fund protokolliert werden.

Firewall

Die Firewall verfügt über 4 Modi („Aus“, „Minimaler Schutz“, „Maximaler Schutz“, „Alle blockieren“) und ist nach der Installation deaktiviert. Somit werden alle Verbindungen akzeptiert. Die Modi können einfach gesetzt werden und eine nützliche Beschreibung informiert den User über das Verhalten der Firewall. Ein kleines Manko ist jedoch, dass kein Regelsatz für die Firewall eingestellt werden kann, d.h. es können keine Ausnahmen hinzugefügt werden.

Diebstahlsicherung

Gleich wie andere Sicherheitsprodukte integriert Kaspersky Mobile Security 9 vier Schutzmechanismen auf ihrem Smartphone, welche standardmäßig deaktiviert sind:



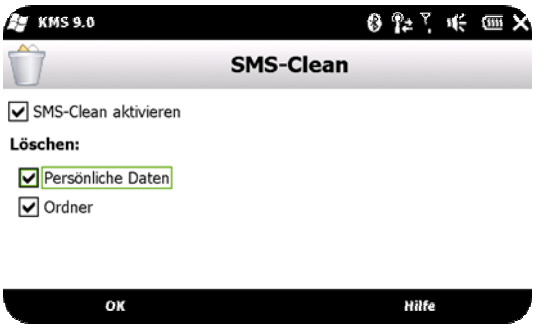
SMS-Block

Mit Hilfe von SMS-Block, hat der User die Möglichkeit, sein Smartphone per Fernsteuerung zu sperren. Hierbei kann eine SMS mit dem Inhalt “Block:” gefolgt von einem Sicherheitscode an das zu blockierende Gerät gesendet werde. Eine Nachricht welche ein möglicher Dieb erhalten soll, kann definiert werden.

Nach einem durchgeführten SMS-Block, konnten keine Notrufnummern mehr gewählt werden. Hier sollte Kaspersky nachbessern, da in der EU auch auf gesperrten Mobiltelefone Notrufnummern erreichbar sein sollten.

SMS-Clean

Usern von Kaspersky Mobile Security 9 ist es möglich, Ordner zu definieren, welche per SMS gelöscht werden können. Hierzu muss der User die Ordner in den Bereich „Zu löschende Ordner“ hinzufügen, des Weiteren kann eingestellt werden, dass Persönliche Daten und/oder die zuvor definierten Ordner gelöscht werden.



SIM-Watch

SIM-Watch erlaubt es dem User, eine Nachricht an eine Telefonnummer bzw. an eine E-Mail Adresse nach einem SIM-Kartentausch zu senden um über die neue Telefonnummer informiert zu werden. Somit kann eine SMS an die erhaltene Nummer gesendet werden, welche zum Beispiel das Smartphone ortet, blockiert oder löscht.

Des Weiteren erlaubt SIM-Watch, dass das Mobiltelefon sofort nach einem SIM-Kartenwechsel blockiert wird und eine Textnachricht angezeigt wird.

GPS-Find

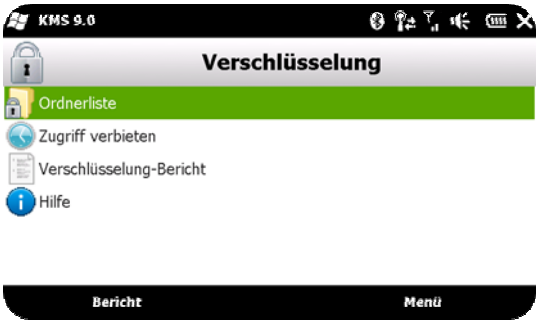
Sollte GPS-Find aktiviert sein, kann das Mobiltelefon per SMS geortet werden. Als Antwort erhält der User eine E-Mail mit einem Link zu Google Maps und der Position des Mobiltelefons an eine zuvor definierte Adresse.

Privatsphäre

Diese Komponente ermöglicht ein Verbergen von sensiblen Informationen. Dazu zählen zum Beispiel Kontakte welche auf der SIM-Karte oder im Gerätespeicher gespeichert sind. Nachrichten und Anrufe können verborgen werden. Wurde zum Beispiel der Kontakt „Max Mustermann“ in die Kontaktliste der Privatsphäre hinzugefügt wird dieser im Telefonbuch, und der Nachrichtenverkehr mit dieser Person verborgen.

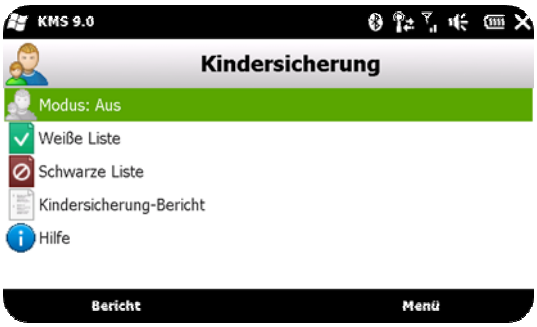
Verschlüsselung

Kaspersky Mobile Security 9 ermöglicht die Verschlüsselung von Ordner, welche nicht zum System gehören. Ebenso wie bei der Privatsphäre können in eine Ordnerliste zu verschlüsselnde Ordner hinzugefügt werden. Je nachdem wenn das Smartphone in den Stromsparmodus wechselt, kann eine Zeitspanne definiert werden, nach deren Ablauf die Daten verschlüsselt werden.



Kindersicherung

Mit Hilfe der Kindersicherung können Regeln für das Senden von SMS und für ausgehende Anrufe definiert werden. Hierbei bietet Kaspersky Mobile Security 9 die Möglichkeit zwischen zwei Modi zu wählen. Der Modus „Weiße Liste“ ermöglicht ein kommunizieren ausschließlich mit Nummer, welche in dieser Liste gespeichert sind (sei es nur Anrufen, nur SMS senden oder beides). Im Modus „Schwarze Liste“ werden Anrufe und SMS an alle Nummern unter Ausnahme dieser Liste erlaubt.



Deinstallation

Die Deinstallation verlief nicht ganz so einfach, da einige zuvor aktivierte Komponenten, wie die Privatsphäre, erst deaktiviert werden müssen. Die Deinstallationsroutine informiert den User jedoch über die zu deaktivierenden Dienste. Positiv aufgefallen ist, dass eine Passworteingabe zur Deinstallation notwendig war, um einem unbefugtem Löschen entgegenzuwirken.

Bedienungsfreundlichkeit

Die Oberfläche für die Konfiguration ist gelungen gestaltet, der User anhand wird von Tooltips unterstützt. Die Tooltips sind einfach verständlich und setzen keinerlei Fachwissen voraus.

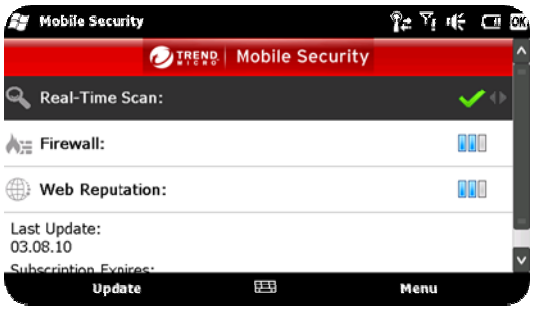
Fazit

Kaspersky Mobile Security 9 ist die ideale Lösung für den verantwortungsbewussten Endanwender und verfügt über eine Vielzahl von durchdachten Diensten zu kleinem Preis. Lediglich 25 Euro pro Smartphone müssen für einen 12-monatigen Schutz investiert werden.

Einen kleinen Minuspunkt erhält die Suite jedoch anhand ihrer Performance. Sind alle Dienste aktiviert, reagierte das Smartphone ein wenig langsamer.

Trend Micro Mobile Security

Trend Micro bietet nun schon die Version 6.5 seiner mobilen Sicherheitssoftware namens Trend Micro Mobile Security an. Die Anwendung ist gut strukturiert und arbeitet verlässlich im Hintergrund. Es integriert die wichtigsten Sicherheitskomponenten wie Diebstahlsicherung, Kindersicherung, Spamschutz für SMS Nachrichten, Browserschutz und eine Firewall.



Installation

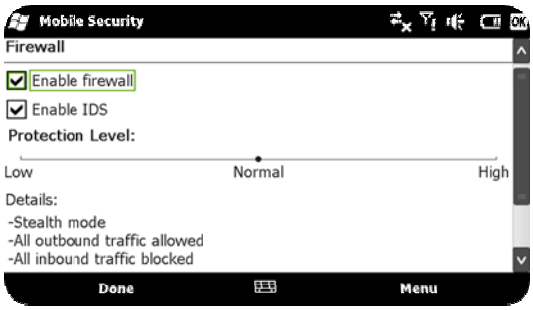
Die Installation von Trend Micro Mobile Security wurde mit Hilfe von ActiveSync durchgeführt. Dazu wurde die Installationsdatei auf das Gerät geladen und ausgeführt. Nach einigen Sekunden wurde das Produkt erfolgreich installiert.

Starten des Programms

Das User Interface von Trend Micro kann direkt über den Home Screen des Mobiltelefons gestartet werden. Die Eingabe eines Passworts ist nicht erforderlich.

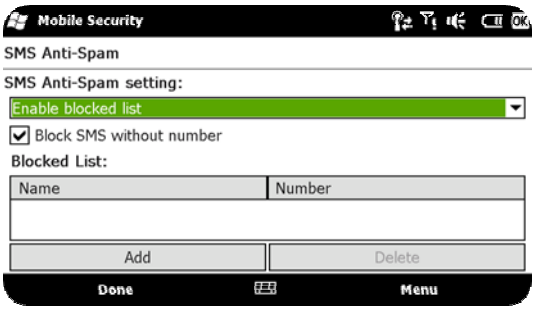
Firewall

Die Firewall ist standardmäßig auf die Sicherheitsstufe „Normal“ gesetzt, welche ausgehenden Internetverkehr erlaubt und eingehenden blockiert. Sie verfügt über zwei weitere Sicherheitsstufen namens „Low“ und „High“, deren Sicherheitseinstellungen in einem Informationsbereich angezeigt werden.



SMS Anti-Spam

Die SMS Anti-Spam Komponente ist in den Grundeinstellungen deaktiviert, kann aber vom User sehr einfach eingeschalten und verwaltet werden. Dazu verwendet Trend Micro Mobile Security das Prinzip einer Black- oder Whitelist, welche der User definieren kann. Entscheidet sich der User eine Blacklist zu verwenden, legt dieser fest von welchen Absendern SMS Nachrichten blockiert werden sollen. Im Falle einer Whitelist, werden all jene Absender blockiert, welche sich nicht in der Liste befinden.

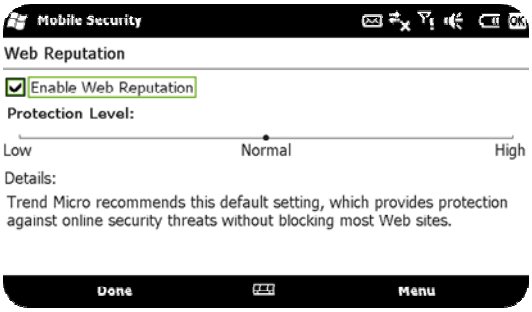


WAP Push Protection

Mit Hilfe der WAP Push Protection Komponente kann eine Liste von vertrauenswürdigen Absender erstellt werden, welchen es erlaubt ist, WAP Push Nachrichten an das Smartphone zu senden. Empfängt das Mobiltelefon eine solche Nachricht von einem Absender, außerhalb der Liste, benachrichtigt Trend Mobile Security den Benutzer. Dieser hat dann die Möglichkeit die Nachricht zu blockieren bzw. zu gestatten.

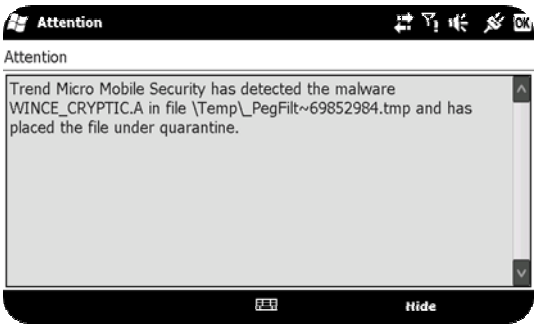
Web Reputation

Web Reputation blockiert Webseiten, welche bereits von Trend Micro als „gefährlich" eingestuft wurden und schützt vor andere online Sicherheitsbedrohungen. Dabei wird der User von Pharming, Phishing, usw. je nach Sicherheitsstufe geschützt. Auch hier kann der User zwischen drei Sicherheitsstufen wählen.



Besucht der User eine Phishing Seite mit aktiviertem Web Reputation, erhält er nach einer erfolgreichen Identifikation durch Trend Micro Mobile Security die folgende Warnung.

Um auch die Virenschutzfunktion von Trend Micro Mobile Security zu testen, wurde der Versuch unternommen das Smartphone zu infizieren. Der Virus wurde jedoch sofort blockiert und in den Quarantäne Ordner verschoben. Anschließend wurde die folgende Warnung angezeigt.



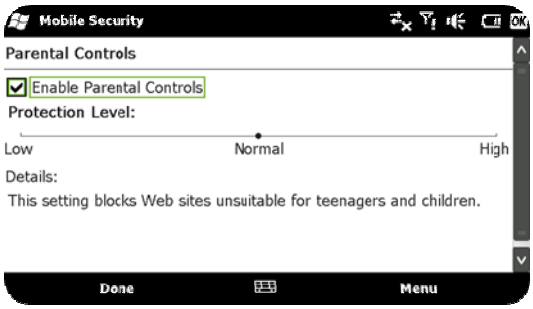
Kindersicherung

Mit Hilfe der Kindersicherung hat der Benutzer die Möglichkeit Sicherheitsstufen zu definieren, welche es Kindern verbietet spezielle Webseiten zu besuchen. Dabei unterscheidet Trend Micro Mobile Security zwischen drei Stufen: „Low", „Normal" und „High".

- „Low" blockiert gewaltsame, pornographische und gefährliche Webseiten

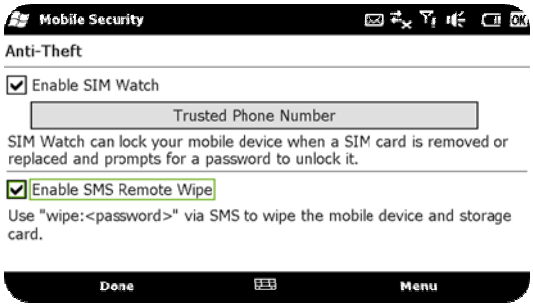
- „Normal“ blockiert für Teenager und Kinder ungeeignete Webseiten
- „High“ blockiert ungeeignete Webseiten für Kinder unter 13 Jahren

Um die Kindersicherung zu aktivieren, muss der Benutzer ein Passwort vergeben, welches anschließend bei Einstellungsänderung der Kindersicherung und Diebstahlsicherung eingegeben werden muss.



Diebstahlsicherung

Die Diebstahlsicherung integriert zwei Sicherheitsfeatures in Ihr Smartphone. Zum einen eine Komponente namens „SIM Watch“, zum anderen die Komponente „SMS Remote Wipe“.



SIM Watch

SIM Watch sperrt das Mobiletelefon nach einem SIM-Kartentausch bzw. nach dem Entfernen der Karte und benachrichtigt den Benutzer. Die Benachrichtigung erfolgt in Form einer SMS an eine vertrauenswürdige Telefonnummer, welche der User beim Aktivieren von SIM Watch definieren muss.

SMS Remote Wipe

Ist SMS Remote Wipe aktiviert, kann der User über eine SMS Nachricht mit dem sein Smartphone und die Speicherkarte ferngesteuert löschen. Dazu muss der User eine SMS Nachricht mit dem Text „wipe:“ gefolgt vom Sicherheitscode an sein Mobiltelefon schicken.

Deinstallation

Die Deinstallation ist problemlos über die Windows Mobile „Programme entfernen“ Routine möglich. Um ein unbefugtes Löschen zu vermeiden, muss das Passwort von Trend Micro Mobile Security eingegeben werden.

Fazit

Trend Micro Mobile Security ist ein sehr übersichtlich gestaltetes Produkt, welches sehr einfach bedient und an die Bedürfnisse des Users angepasst werden kann. Es integriert die derzeit wichtigsten Sicherheitsfeatures, jedoch verfügt es über keinen Ortungsservice.

Trend Micro ist auch das einzige Produkt, das eine sehr abgespeckte Variante für das iPhone im Angebot hat.

Fazit

Gerade in der heutigen Zeit, sollte niemand der ein Smartphone benützt, auf Sicherheitssoftware verzichten. Nicht nur wegen der Risiken im Umgang mit dem Internet, sondern auch - oder vor allem - wegen anderer Bedrohungen, wie Diebstahl oder Datenspionage. Wirklich jedes Smartphone sollte ausreichend geschützt werden, im privaten und betrieblichen Bereich.

Aufgrund der guten Prozessorleistung moderner Geräte ist eine Minderung der Performance oder der Batterielaufzeit so gut wie nicht erkennbar.

Die von uns getesteten Produkte erfüllten alle ihren Zweck, jedoch ist die Entscheidung welches Produkt für welchen User geeignet ist, schwierig.

ESET Mobile Security ist ein übersichtlich gestaltetes Antiviren Produkt, welches sehr einfach bedient werden kann. Für Benutzer, die mehrere SIM-Karten verwenden und nicht auf einen Diebstahlschutz verzichten wollen, hat ESET eine elegante Lösung gefunden.

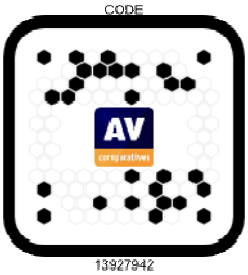
Mit **F-Secure Mobile Security** ist ihr Smartphone von Dieben und Malware geschützt, da es über die derzeit wichtigsten Sicherheitskomponenten verfügt. Es kann sehr einfach direkt über die Homepage bezogen und installiert werden.

Kaspersky Mobile Security ist die ideale Lösung für den verantwortungsbewussten Endanwender und verfügt über eine Vielzahl von durchdachten Diensten zu kleinem Preis.

Trend Micro Mobile Security ist übersichtlich gestaltet und auch für das iPhone verfügbar. Mit Hilfe der Web Reputation Komponente wird ihr Smartphone schon bevor eine gefährliche Webseite geöffnet wird geschützt.

Man sollte genau abwägen, welche Schutzmechanismen gebraucht werden, und sich dann für das dementsprechende Produkt entscheiden. Kostenlose Testversionen stellen fast alle Anbieter per Download zur Verfügung. Zu empfehlen wäre auf jeden Fall ein Produkt, welches Virenschutz, Firewall, Phishing-Filter und eine Remote Sperre anbietet, um ausreichend geschützt zu sein.

Alle Produkte erfüllen Ihre Pflichten gut und können mit dem „Approved Zertifikat“ ausgezeichnet werden.



Besondere Vorsicht ist bei der Verwendung von Tag-Readern geboten. Wir beobachten immer häufiger missbräuchliche Verwendung auf Events. Vor allem bei Großereignissen wie Konzerten werden Beetagg, QR-Code und Datamatrix illegal plakatiert, um auf Phishing- und Malwareseiten zu verlinken. Ein guter Phishing-Filter ist hier die beste technische Lösung.

Feature Liste Mobile Security

Windows Mobile

Product name	*ESET Mobile Security*	*F-Secure Mobile Security*	*Kaspersky Mobile Security*	*Trend Micro Mobile Security*
Supported OS versions	Windows Mobile 5.0-6.5	Windows Mobile 5.0-6.5	Windows Mobile 5.0-6.5	Windows Mobile 5.0-6.5
Supported Program languages	English	English, Arabic, Simplified Chinese, Traditional Chinese, Danish, Spanish, Finnish, French, German, Bahasa Indonesia, Italian, Japanese, Bahasa Malaysia, Dutch, Norwegian, Polish, Brazilian Portuguese, Portuguese, Russian, Swedish, Tagalog, Thai, Turkish, Korean	English, Russian, German, French, Italian, Polish, Spanish, Portuguese, Danish, Norwegian, Finnish, Swedish, Simplified Chinese, Traditional Chinese, Arabic, Turkish, Czech, Dutch	English, German, Spanish, French, Russian, Traditional Chinese, Dutch
Locking Features				
Lock Contacts	-	YES	YES	-
Lock Images/Files	-	YES	YES	-
Lock SMS/MMS	-	YES	YES	YES
Lock SIM	-	YES	YES	-
Anti Spam Features				
Whitelist/Blacklist calls	-	-	YES	-
Whitelist/Blacklist SMS	YES	-	YES	YES
Whitelist/Blacklist MMS	YES	-	-	YES
Block known SMS/MMS spam	YES	-	-	YES
mark as spam with one click	-	-	YES	-
White- and Blacklisting with wildcards	-	-	YES	-
Block attachments/applications/file extensions	YES	-	-	-
Parental Control				
Pay Number locking	-	-	YES	-
SMS Find (Localization of the Smartphone)	-	YES	YES	-
Log visited URLs	-	-	-	YES
Firewall Features				
Real-Time protection of inbound/outbound Traffic	YES	YES	YES	YES
App Whitelisting/Blacklisting	YES	-	-	-
Learning features	YES	-	-	-
Different protection level	YES	YES	YES	YES
Different rule sets	YES	YES	-	YES
WiFi / Bluetooth protection	YES	YES	YES	-
Activity log	YES	YES	-	YES
Protection log	YES	YES	YES	YES
Customizable firewall rules	YES	YES	YES	YES
Stateful packet inspection (conditional rules)	YES	YES	-	YES
Remote Features				
Remote wipe of a stolen Smartphone	YES	YES	YES	YES
Remote wipe with Exchange Server 2007/2010 / Outlook Web Access / ActiveSync	YES	Through the management portal and device management	-	-
Remote GPS localization	-	YES	YES	-
SIM Watch (changing the SIM)	YES	YES	YES	YES

Product name	*ESET Mobile Security*	*F-Secure Mobile Security*	*Kaspersky Mobile Security*	*Trend Micro Mobile Security*
Remote installation	-	Through device management or through F-Secure Mobile Services portal	in the enterprise version	YES
Remote configuration	-	Through device management	in the enterprise version	YES
Remote updates	YES	YES	-	YES
Remote encryption	-	-	-	YES
Encryption Features				
File System encryption	-	Through partner solution	YES	YES
Password protected encryption	-	Through partner solution	YES	YES
Encryption by data types (Outlook, Word, Excel, PDF, etc.) and by data location (on device, attached, memory card, etc.)	-	Through partner solution	only by data location	YES
Admin decrypting option without password	-	Through partner solution	-	YES
Authentication				
Policy controlled authentication	-	-	-	YES
Access & encryption control	-	-	YES	YES
Port control: USB, Memory Cards, Bluetooth, WiFi	-	YES	-	YES
Resource Access control: IR, Camera, voice recording	-	-	-	YES
Password policy: strength, length, etc.	-	YES	YES	YES
Maximum number of failed attempts	-	YES	-	YES
Grace period	-	YES	YES	-
Lock Screen with password protection	-	YES	YES	YES
AV Features				
File protection	YES	YES	YES	YES
Network protection	YES	YES	-	YES
SMS/MMS Scanner	YES	YES	YES	Partial, Blacklist/Whitelist & Attachment Scan
Email Scanner	YES	YES	YES	-
Different Update profiles	YES	YES	in the enterprise version	YES
Own roaming update profile	YES	YES	YES	YES
Scan inside archives	YES	YES	YES	YES
Prevent access to harmful web sites (malware and phishing sites)	-	YES	-	YES
Anti-Theft Features				
Report thief's location at SIM change	-	YES	-	YES
Report thief's phone number by SMS	YES	YES	YES	YES
Possibility to receive calls while locked	-	YES	-	YES
Possibility to make emergency calls while locked	-	YES	-	YES
Support				
Email Support	YES	YES	YES	YES
Online Help	YES	YES	YES	YES
Online Help (special URL designed for browsing with the phone)	-	YES	YES	YES
User manual	YES	YES	YES	YES
User Forum	-	-	YES	YES
Online Chat	-	-	-	YES
Support over Telephone	YES	YES	YES	YES
Supported languages (of support)	all	all	all	all

Product name	*ESET Mobile Security*	*F-Secure Mobile Security*	*Kaspersky Mobile Security*	*Trend Micro Mobile Security*
Price (depends from channels etc.)				
Price 1 phone / 1 year	25 EUR	35 EUR	25 EUR	25 EUR
Price 3 phones / 2 years	61 EUR	180 EUR	150 EUR	150 EUR
Various				
Direct Install on Device through Download-Link	YES	YES	YES	YES
PC Management Software	-	-	-	YES
Central Management Software	-	Through F-Secure Mobile Services portal available for the administrators	in the enterprise version	YES
Synchronizing	YES	-	-	-
PC Application Install	YES	Possible through ActiveSync	YES	YES
Updates thru PC	YES	Possible through ActiveSync	Possible through ActiveSync	YES
Offline activation	-	-	-	YES
No SIM activation	YES	YES	YES	YES
Updates (Auto/On-Demand)	YES	YES	YES	YES
Quarantine	YES	YES	YES	YES
Blocking roaming data	YES	-	YES	-
SIM Matching	YES	-	-	YES
Statistics	YES	YES	in the enterprise version	YES

Symbian				
Product name	***ESET Mobile Security***	***F-Secure Mobile Security***	***Kaspersky Mobile Security***	***Trend Micro Mobile Security***
Supported OS versions	S60 3rd/5th edition (Symbian 9.1-9.4)	S60 3rd/5th edition (Symbian 9.1-9.4)	S60 3rd/5th edition (Symbian 9.1-9.4)	S60 3rd/5th edition (Symbian 9.1-9.4)
Supported Program languages	English	English, Arabic, Simplified Chinese, Traditional Chinese, Danish, Spanish, Finnish, French, German, Bahasa Indonesia, Italian, Japanese, Bahasa Malaysia, Dutch, Norwegian, Polish, Brazilian Portuguese, Portuguese, Russian, Swedish, Tagalog, Thai, Turkish, Korean	English, Russian, German, French, Italian, Polish, Spanish, Portuguese, Danish, Norwegian, Finnish, Swedish, Simplified Chinese, Traditional Chinese, Arabic, Turkish, Czech, Dutch	English, German, Spanish, French, Russian, Traditional Chinese, Dutch
Locking Features				
Lock Contacts	-	YES	YES	-
Lock Images/Files	-	YES	YES	-
Lock SMS/MMS	-	YES	YES	-
Lock SIM	-	YES	YES	-
Anti Spam Features				
Whitelist/Blacklist calls	-	-	YES	-
Whitelist/Blacklist SMS	YES	-	YES	YES
Whitelist/Blacklist MMS	YES	-	-	-
Block known SMS/MMS spam	YES	-	-	YES
mark as spam with one click	-	-	YES	-
White- and Blacklisting with wildcards	-	-	YES	-
Block attachments/applications/file extensions	YES	-	-	-
Parental Control				
Pay Number locking	-	-	YES	-
SMS Find (Localization of the Smartphone)	-	YES	YES	-
Log visited URLs	-	-	-	YES
Firewall Features				
Real-Time protection of inbound/outbound Traffic	YES	YES	YES	YES

Product name	*ESET Mobile Security*	*F-Secure Mobile Security*	*Kaspersky Mobile Security*	*Trend Micro Mobile Security*
App Whitelisting/Blacklisting	-	-	-	-
Learning features	-	-	-	-
Different protection level	YES	YES	YES	YES
Different rule sets	YES	YES	-	YES
WiFi / Bluetooth protection	YES	YES	YES	-
Activity log	YES	YES	-	YES
Protection log	YES	YES	YES	YES
Customizable firewall rules	YES	YES	YES	YES
Stateful packet inspection (conditional rules)	YES	YES	-	YES
Remote Features				
Remote wipe of a stolen Smartphone	YES	YES	YES	YES
Remote wipe with Exchange Server 2007/2010 / Outlook Web Access / ActiveSync	YES	Through the management portal and device management	-	-
Remote GPS localization	-	YES	YES	-
SIM Watch (changing the SIM)	YES	YES	YES	YES
Remote installation of the Security System	-	Through device management or through F-Secure Mobile Services portal	in the enterprise version	YES
Remote configuration	-	Through device management	in the enterprise version	YES
Remote updates	YES	YES	-	YES
Remote encryption	-	-	-	YES
Encryption Features				
File System encryption	-	Through partner solution	YES	YES
Password protected encryption	-	Through partner solution	YES	YES
Encryption by data types (Outlook, Word, Excel, PDF, etc.) and by data location (on device, attached, memory card, etc.)	-	Through partner solution	only by data location	YES
Admin decrypting option without password	-	Through partner solution	-	YES
Authentication				
Policy controlled authentication	-	-	-	YES
Access & encryption control	-	-	YES	YES
Port control: USB, Memory Cards, Bluetooth, WiFi	-	YES	-	-
Resource Access control: IR, Camera, voice recording	-	-	-	-
Password policy: strength, length, etc.	-	YES	YES	YES
Maximum number of failed attempts	-	YES	-	YES
Grace period	-	YES	YES	-
Lock Screen with Password protection	-	YES	YES	YES
AV Features				
File protection	YES	YES	YES	YES
Network protection	YES	YES	-	YES
SMS/MMS Scanner	YES	YES	YES	Partial, Blacklist/ Whitelist+ Attachment Scan
Email Scanner	YES	YES	YES	-
Different Update profiles	YES	YES	in the enterprise version	YES
Own roaming update profile	-	YES	YES	YES
Scan inside archives	YES	YES	YES	YES
Prevent access to harmful web sites (malware and phishing sites)	-	YES	-	YES
Anti-Theft Features				
Report thief's location at SIM change	-	YES	-	YES
Report thief's phone number by SMS	YES	YES	YES	YES
Possibility to receive calls while locked	-	YES	-	YES
Possibility to make emergency calls while locked	-	YES	-	YES
Support				
Email Support	YES	YES	YES	YES
Online Help	YES	YES	YES	YES

Product name	*ESET Mobile Security*	*F-Secure Mobile Security*	*Kaspersky Mobile Security*	*Trend Micro Mobile Security*
Online Help (special URL designed for browsing with the phone)	-	YES	YES	YES
User manual	YES	YES	YES	YES
User Forum	-	-	YES	YES
Online Chat	-	-	-	YES
Support over Telephone	YES	YES	YES	YES
Supported languages (of support)	all	all	all	all
Price (depends from channels etc.)				
Price 1 phone / 1 year	25 EUR	35 EUR	25 EUR	25 EUR
Price 3 phones / 2 years	61 EUR	180 EUR	150 EUR	150 EUR
Various				
Direct Install on Device through Download-Link	YES	YES	YES	YES
PC Management Software	-	-	-	YES
Central Management Software	-	Through F-Secure Mobile Services portal available for the administrators	Possible through ActiveSync	YES
Synchronizing	YES	-	-	-
PC Application Install	YES	Possible through PC suite	YES	YES
Updates thru PC	YES	Possible through PC suite	in the enterprise version	YES
Offline activation	-	-	-	YES
No SIM activation	YES	Yes. The functionality depends on the variant	YES	YES
Updates (Auto/On-Demand)	YES	YES	YES	YES
Quarantine	YES	YES	YES	YES
Blocking roaming data	YES	-	YES	-
SIM Matching	YES	-	-	YES
Statistics	YES	YES	in the enterprise version	YES
PW protection of uninstallation	YES	-	YES	YES

	Android	Android	iPhone
Product name	***F-Secure Mobile Security***	***Trend Micro Mobile Security Suite***	***Trend Micro SmartSurfing***
Supported OS versions	Android 1.6 and above	Android 2.x	iOS 3.1 and above
Supported Program languages	English, Arabic, Simplified Chinese, Traditional Chinese, Danish, Spanish, Finnish, French, German, Bahasa Indonesia, Italian, Japanese, Bahasa Malaysia, Dutch, Norwegian, Polish, Brazilian Portuguese, Portuguese, Russian, Swedish, Tagalog, Thai, Turkish, Korean	English	English
Locking Features			
Lock Contacts	YES	-	-
Lock Images/Files	YES	-	-
Lock SMS/MMS	YES	-	-
Lock SIM	YES	-	-
Anti Spam Features			
Whitelist/Blacklist calls	-	YES	-
Whitelist/Blacklist SMS	-	YES	-
Whitelist/Blacklist MMS	-	YES	-
Block known SMS/MMS spam	-	YES	-
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)	YES	-	-
Log visited URLs	-	YES	YES

Product name	*F-Secure Mobile Security*	*Trend Micro Mobile Security Suite*	*Trend Micro SmartSurfing*
Firewall Features			
Real-Time protection of inbound/outbound Traffic	-	-	-
App Whitelisting/Blacklisting	-	-	-
Learning features	-	-	-
Different protection level	-	-	-
Different rule sets	-	-	-
WiFi / Bluetooth protection	-	-	-
Activity log	-	-	-
Protection log	-	-	-
Customizable firewall rules	-	-	-
Stateful packet inspection (conditional rules)	-	-	-
Remote Features			
Remote wipe of a stolen Smartphone	YES	-	System provided
Remote wipe with Exchange Server 2007/2010 / Outlook Web Access / ActiveSync	Remote wipe is enabled through the management portal	-	System provided
Remote GPS localization	YES	-	-
SIM Watch (changing the SIM)	YES	-	-
Remote installation of the Security System	Through device management or through F-Secure Mobile Services portal	-	-
Remote configuration	-	-	System provided
Remote updates	YES	-	-
Remote encryption	-	-	-
Encryption Features			
File System encryption	Through partner solution	-	System provided or vault
Password protected encryption	Through partner solution	-	System provided
Encryption by data types (Outlook, Word, Excel, PDF, etc.) and by data location (on device, attached, memory card, etc.)	Through partner solution	-	-
Admin decrypting option without password	Through partner solution	-	-
Authentication			
Policy controlled authentication	-	-	System provided
Access & encryption control	-	-	System provided
Port control: USB, Memory Cards, Bluetooth, WiFi	-	-	System provided
Resource Access control: IR, Camera, voice recording	-	-	System provided
Password policy: Strength, length, etc.	Partially. Antitheft uses system locking functionalities.	-	System provided
Maximum number of failed attempts	YES	-	System provided
Grace period	YES	-	System provided
Lock Screen with Password protection	YES	-	System provided
AV Features			
File protection	YES	YES	-
Network protection	YES	-	-
SMS/MMS Scanner	-	-	-
Email Scanner	The attachments are scanned on the memory card	-	-
Different Update profiles	YES	YES	-
Own roaming update profile	YES	YES	-
Scan inside archives	YES	-	-
Prevent access to harmful web sites (malware and phishing sites)	YES	YES	YES
Anti-Theft Features			
Report thief's location at SIM change	YES	YES	-
Report thief's phone number by SMS	YES	-	-
Possibility to receive calls while locked	YES	YES	-
Possibility to make emergency calls while locked	YES	YES	-

Product name	***F-Secure Mobile Security***	***Trend Micro Mobile Security Suite***	***Trend Micro SmartSurfing***
Support			
Email Support	YES	YES	YES
Online Help	YES	YES	YES
Online Help (special URL designed for browsing with the phone)	YES	YES	YES
User manual	YES	YES	YES
User Forum	-	YES	YES
Online Chat	-	YES	YES
Support over Telephone	YES	YES	-
Supported languages (of support)	all	all	all
Price (depends from channels etc.)			
Price 1 phone / 1 year	35 EUR	N/A	free
Price 3 phones / 2 years	180 EUR	N/A	free
Various			
Direct Install on Device through Download-Link	YES	YES	YES
PC Management Software	-	-	-
Central Management Software	Through F-Secure Mobile Services portal available for the administrators	-	-
Synchronizing	-	-	-
PC Application Install	From PC user can install using e.g. HTCSync and also using adb that comes with the development tools.	YES	YES
Updates thru PC	-	-	-
Offline activation	-	YES	YES
No SIM activation	Yes. The functionality depends on the variant	-	-
Updates (Auto/On-Demand)	YES	YES	-
Quarantine	-	-	-
Blocking roaming data	-	-	-
SIM Matching	-	-	-
Statistics	YES	YES	-
PW protection of uninstallation	-	-	-

Copyright and Disclaimer

This publication is Copyright © 2010 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (August 2010)