

Kaspersky

Endpoint Security

für Smartphones

Kaspersky Endpoint Security für Smartphones schützt vertrauliche Daten auf mobilen Endgeräten im Firmeneinsatz vor Diebstahl, Verlust, unerlaubtem Zugriff und mobiler Schadsoftware.

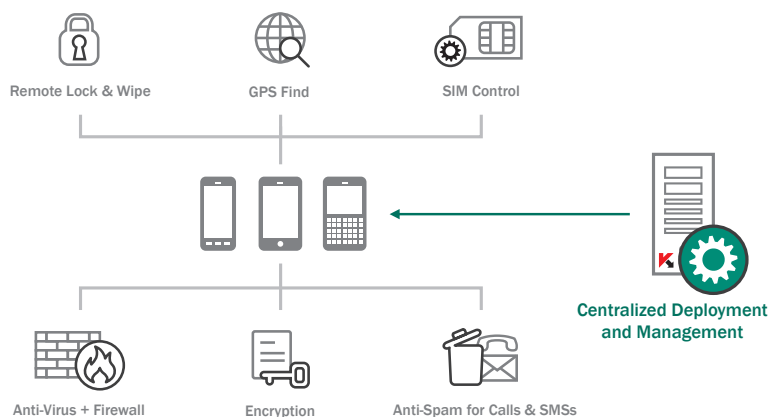
Kaspersky Endpoint Security für Smartphones wurde entwickelt, um Sicherheitslücken zuverlässig zu schließen. Die Schutzsoftware kann sich aus der Ferne mit dem Endgerät verbinden und es bei Verlust oder Diebstahl gegen Schadsoftware schützen und die wertvollen Daten auf dem Gerät verschlüsseln.

Heute müssen Mitarbeiter in vielen Unternehmen jederzeit online erreichbar sein, nicht nur im Büro, sondern auch unterwegs. Fast immer wird dafür ein Smartphone eingesetzt. Anrufe, Nachrichten, Zugang zum Firmennetz und zum Internet – Smartphone erlauben die vollständige Vernetzung im Taschenformat. Als Resultat können auf den mobilen Geräten große Mengen von wertvollen, geschäftskritischen Informationen gespeichert sein. Das macht sie zu attraktiven Angriffszielen für Kriminelle und kann zum Verlust von Firmeninformationen, unerlaubtem Zugriff und Infektionen mit Schadsoftware führen.

Die kompakten Smartphones gehen leicht verloren und werden schnell gestohlen. Viele tragbare Endgeräte werden in Restaurants oder Cafés, in Taxis und Flugzeugen vergessen sowie an belebten Orten entwendet. Jedes dieser Geräte kann vertrauliche E-Mails, Kundendaten, Finanzinformationen sowie persönliche Daten wie Zugangscodes für das Online-Banking und mehr enthalten.

Tragbare Endgeräte werden häufig nicht vor mobiler Schadsoftware geschützt, da diese Bedrohung weniger bekannt ist als Schadsoftware für den PC. Diese Vernachlässigung kann gefährlich sein, da es mittlerweile für jede gebräuchliche Smartphone-Plattform entsprechende Schadsoftware gibt. Sie kann das Endgerät eines Anwenders leicht infizieren und dann beispielsweise beginnen, heimlich SMS-Nachrichten an eine Premium-Nummer zu senden und so finanziellen Schaden anrichten. Andere Schadprogramme sind darauf ausgerichtet, Nutzerdaten für Online-Betrug zu sammeln. Die Risiken, wenn beruflich genutzte Smartphones ungeschützt bleiben, umfassen:

- Bekanntwerden vertraulicher Firmendaten, wenn das Gerät gestohlen oder verloren wird
- Missbrauch von Firmeninformationen bei unerlaubtem Zugriff auf das Endgerät
- Angriffe durch mobile Schadsoftware und andere Crimeware



Kaspersky Lab ist weltweit der größte nicht börsennotierte Anbieter von Sicherheitslösungen.

Unsere Produkte schützen Heimanwender und Unternehmen jeder Größenordnung umfassend vor allen Arten von Internetbedrohungen, darunter Viren, Spyware, Hacker-Angriffe und Spam.

Aktuell bieten unsere Lösungen mehr als 300 Millionen Systemen rund um die Welt Schutz. Die von Kaspersky Lab entwickelten Technologien finden sich außerdem in den Produkten und Services von rund 100 führenden Anbietern von IT-, Netzwerk- und Kommunikationslösungen der IT-Branche wieder.

FUNKTIONEN DER SOFTWARE

- Verschlüsselungslösung mit Schutz vor Diebstahl und Viren
- Einfache Verteilung der Software „over-the-air“ mittels eigener Managementlösung oder Software von Drittanbietern
- Umfangreiche Einstellungen und Beschränkungen möglich – über das Kaspersky Administration Kit, Sybase Afaria oder den Microsoft System Center Mobile Device Manager
- Unterstützt wichtige Smartphone-Plattformen: Android, BlackBerry, Symbian sowie Symbian^3 (nur Nokia) und Windows Mobile

Wie schützt Kaspersky Endpoint Security für Smartphones mobile Anwender?

- **Anti-Diebstahl:** Das Smartphone kann bei Diebstahl oder Verlust aus der Ferne gesperrt, gelöscht und über GPS verfolgt werden.
- **SIM Watch:** Selbst wenn der Dieb die SIM-Karte austauscht, bleiben die Funktionen zum Fernzugriff erhalten. Die neue Nummer wird per SMS zum rechtmäßigen Besitzer geschickt.
- **Verschlüsselung:** Dateien, Ordner und Speicherkarten können verschlüsselt und der Zugriff auf sie per Passwort geschützt werden.
- **Anti-Virus:** Schutz in Echtzeit, Scans bei Zugriff und nach Zeitplan, automatische Updates der Antiviren-Datenbank „over-the-air“.
- **Anti-Spam für Anrufe und SMS:** Unerwünschte Anrufe und Nachrichten lassen sich einfach ausfiltern.
- **Schutz der Privatsphäre** durch das Verbergen von Kommunikationsdetails bei bestimmten Kontakten einschließlich Adressbucheinträgen, Anruflisten und SMS.

Management

Mit Kaspersky Endpoint Security für Smartphones behält die IT-Abteilung die volle Kontrolle über die im Umlauf befindlichen Smartphones. Die Admins definieren unter anderem, welche Funktionen freigegeben oder abgeschaltet sind, welche Einstellungen Nutzer selbst verändern dürfen, sowie die Häufigkeit der Antiviren-Updates.

Unterschiedlichen Benutzergruppen können unterschiedliche Richtlinien zugewiesen werden. Die Richtlinien werden nahtlos „over-the-air“ synchronisiert. Administratoren haben die Möglichkeit, folgende Einstellungen zu konfigurieren:

- **Anti-Virus:** Welche Dateitypen werden untersucht und welche werden immer vom Scan ausgenommen, was soll bei der Entdeckung von Schadsoftware passieren (Löschen, Quarantäne, Log-Eintrag, Benutzeranfrage), Updatehäufigkeit der Antiviren-Datenbank.
- **Anti-Diebstahl:** Welche Komponenten sind freigegeben oder abgeschaltet (Blockieren, Datenlöschung, GPS Find, SIM Watch), welche E-Mails und Telefonnummern werden für die Benachrichtigung bei Problemen genutzt, sowie detaillierte Einstellungen für jede Komponente.
- **Verschlüsselung:** Welche Ordner sollen verschlüsselt werden?
- **Anti-Spam:** Ist diese Funktion für Anrufe, SMS und Datenschutz eingeschaltet?
- **Synchronisation:** Wie oft soll sich das Produkt mit dem Management-Server verbinden.

Die IT-Abteilung kann durch Richtlinien für jedes der aufgeführten Features festlegen, ob die Anwender Einstellungen selbst verändern dürfen oder nicht.

SYSTEMANFORDERUNGEN

Unterstützte Smartphones

- Android 1.5 bis 2.3
- BlackBerry 4.5 bis 6.0
- Symbian S60 9.1 bis 9.4, Symbian^3 (nur Nokia)
- Windows Mobile 5.0 bis 6.5

Managementplattformen

- Kaspersky Administration Kit 8.0 (ab Version 8.0.2121)
- Microsoft System Center Mobile Device Manager 2008 SP1
- Sybase Afaria 6.5

Bereitstellung

Kaspersky Endpoint Security für Smartphones kann „over-the-air“ problemlos an mehrere Endgeräte verteilt werden. Die Installation läuft für die Anwender ohne Störung oder Nutzereingaben ab. Das Produkt kann über die folgenden Plattformen verteilt und verwaltet werden:

- Microsoft System Center Mobile Device Manager
- Sybase Afaria
- Kaspersky Administration Kit

Besuchen Sie www.kaspersky.de, um mehr über die Anwendung zu erfahren.

Kaspersky Endpoint Security 8 für Smartphones kann als Bestandteil von Kaspersky Open Space Security erworben werden.

Eine Liste der Partner von Kaspersky Lab ist hier verfügbar: www.kaspersky.de/partner_finden

Juni 2011

Kaspersky Labs GmbH
Despag-Strasse 3
85055 Ingolstadt
Deutschland
www.kaspersky.de
E-Mail: DEBusiness@kaspersky.de
Telefon +49 (0) 841 98 189 590
Telefax +49 (0) 841 98 189 100

Kaspersky Labs GmbH
Wienerbergstrasse 11/12a
1100 Wien
Österreich
www.kaspersky.at
E-Mail: teamaustria@kaspersky.at
Telefon +43 (0) 1 99 460 6400
Telefax +43 (0) 1 99 460 5000

Kaspersky Labs GmbH
Allmendstrasse 1
6312 Steinhausen/Zug
Schweiz
www.kaspersky.ch
E-Mail: teamswiss@kaspersky.ch