

# Kaspersky<sup>®</sup> Mobile Security

## Enterprise Edition

What is your smart phone worth? Chances are the data on the phone is worth far more than the device itself. Kaspersky Mobile Security Enterprise Edition is designed specifically for protecting data by defending corporate mobile users from malicious programs, SMS spam and Internet attacks. It also protects confidential data should the device be lost or stolen.

Why is it necessary to protect corporate smartphones? Mission-critical business data can be damaged or stolen by malware written specifically to target smartphones. A smartphone can fall victim to Internet attacks when downloading information from the Internet. Infected mobile devices can be used to penetrate the network perimeter of a corporate IT system. The loss or theft of a smartphone can leave sensitive corporate information in nefarious hands. In addition, SMS spam is more than just an inconvenience. It is increasingly popular for introducing malware and other Internet-borne attacks.

While mobile devices such as smart phones are clearly necessary for business productivity and efficiency, they come with risk. Kaspersky Mobile Security Enterprise Edition is designed to help companies mitigate these risks. Leveraging the latest technology for mobile platforms with Kaspersky Lab's extensive experience in combating malware, hacker attacks and spam; the solution provides comprehensive protection for corporate smartphones and the data that resides on them. Kaspersky Mobile Security Enterprise Edition is now fully supported by Kaspersky Administration Kit, empowering system administrators with centralized security management of any network node, whether it is a file server, a workstation, or a mobile device.

### Easy to deploy

Kaspersky Mobile Security Enterprise Edition can be installed from a single administration station, regardless of the number of mobile devices or where they are located. The system can be installed:

Locally, via a PC using Microsoft ActiveSync or Nokia PC Suite or it can be installed remotely, via an SMS message link from the Administration Kit (enabled with a GSM modem).

### Flexible administration

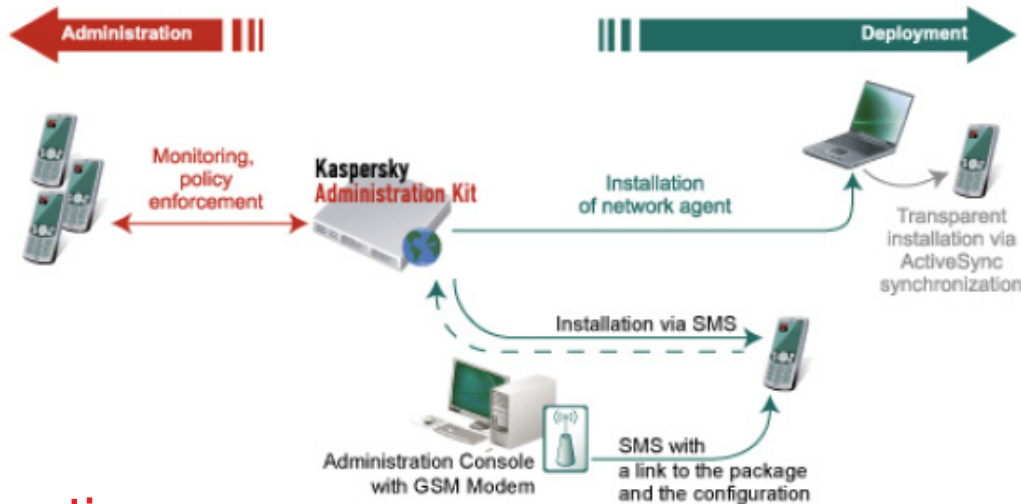
In the event of a virus epidemic or a specific threat, the system administrator can respond by adjusting device security parameters for all users, or for a specific group. User settings can be restricted to ensure compliance with security policies.



## Complete control

Regardless of where the user is, you always have full control over their mobile device's security. When a device has Internet access, it will automatically establish a connection with the Administration Kit for updates and application of any new policies that have been established by the system administrator.

The system administrator can draw information on any device at any time, including time of the most recent connection, status of antivirus and anti-spam protection, and reports from the Anti-Theft and Firewall modules.



## Functions

**Anti-Theft protection.** In the event a smartphone is lost or stolen, a user or system administrator can protect the data by remotely blocking the smartphone or deleting files, messages, and contact lists. The user can also find out who the "new owner" of the lost device is.

- **SMS Block.** If a smartphone is lost, the user can send a "hidden SMS message" to the original SIM card. Access to the smartphone will be blocked until a pre-set password is entered.
- **SMS Clean.** This function is similar to the SMS Block feature, but instead of blocking the smartphone it cleans the device's memory.
- **SIM Watch.** If a smartphone is stolen, the "new owner" will most probably replace the original SIM card. The SIM Watch function will prevent the "new owner" from accessing any personal data without the initial SIM card inserted in the device. When the initial SIM card is replaced with a new one, the SMS Watch function will send the original user the new telephone number of the device without the "new owner's" knowledge.

**Antivirus protection.** Kaspersky Mobile Security provides real-time anti-malware scanning of all incoming files and connections to keep you free of malicious programs. The system administrator can also implement regular scanning at a pre-determined time. If an infected object is detected and cannot be disinfected, it is stored in the quarantine folder or deleted.

**Firewall.** The system administrator can select one of the integrated IP firewall protection levels. Depending on the level selected, one or more restrictions will be applied to provide user security.

**Anti-Spam for SMS.** Telephone numbers of known spam sources, sender names, unwanted words or phrases can be added to a blacklist to ensure that such messages are always blocked. The user can also add addresses from the contact list to a whitelist to allow all messages from specific senders.

**Automatic updates.** Antivirus databases are updated automatically at intervals set by the system administrator. Updates are available via WAP/HTTP (GPRS, EDGE, Wi-Fi, etc.) or via a PC.

### System requirements

#### Hardware requirements

- Windows Mobile 5.0, 6.0, 6.1
- Symbian 9.1, 9.2 Series 60 3rd (Nokia only)

For more information, please contact:

Kaspersky Lab Americas  
500 Unicorn Park  
Woburn, MA 01801  
866-563-3099  
www.kaspersky.com

Copyright © 2008 Kaspersky Lab, Ltd.

Kaspersky® Anti\_Virus and Kaspersky® Security are registered trademarks of Kaspersky Lab Ltd. All other names and trademarks are the copyrighted work of their respective owners.

