

▶ KASPERSKY SECURITY FOR MOBILE

Increased management visibility and security for mobile endpoints — without the complexity of a separate solution.

Deploying, managing and securing your mobile IT environment need not be complicated or expensive. **Mobile Device Management (MDM)** makes the secure configuration of mobile devices painless and straightforward, while a **mobile agent** is installed on the device to provide the protection you need against today's threats — even on employee-owned devices!

Key features:

- SUPPORT FOR TABLETS AND SMARTPHONES
- OVER THE AIR PROVISIONING (OTA)
- TIME-PROVEN, AGENT BASED MOBILE SECURITY
- SECURELY IMPLEMENTS APPLE MDM AND MICROSOFT EXCHANGE ACTIVESYNC
- NATIVE INTEGRATION WITH KASPERSKY SECURITY CENTER FOR CONFIGURATION, CONTROL, REPORTING, INVENTORIES AND POLICY SETTING

Mobile platforms supported:

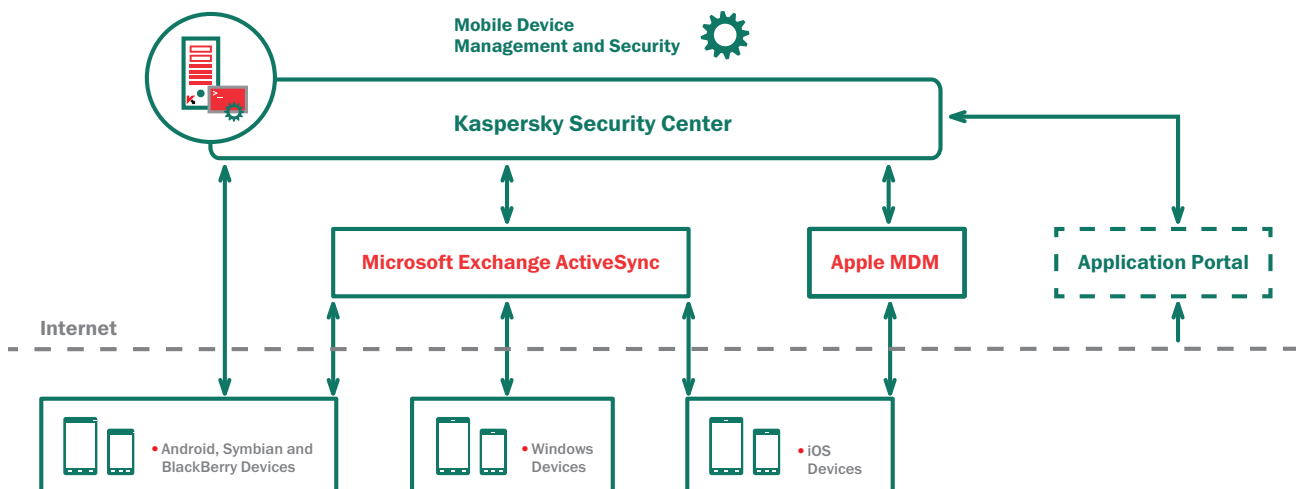
- iOS
- ANDROID™
- WINDOWS® PHONE
- WINDOWS MOBILE
- BLACKBERRY®
- SYMBIAN

▶ PERFECT FOR “BRING YOUR OWN DEVICE” (BYOD) INITIATIVES

Many employees use their own devices for both personal and corporate tasks. In fact, some organizations encourage workers to choose their preferred smartphone or tablet from a retailer, and IT adds email and corporate access to the employee-owned device.

There are savings and productivity benefits, but BYOD can also open the organization to security risks. Corporate data, improperly secured and potentially co-mingled with personal items, can be easily exploited. Often these devices are also used by family members with no regard for application security. Some are even rooted or jailbroken.

Kaspersky Security for Mobile solves these problems by enabling secure configuration and deployment of smartphones and tablets using the same console as your network security. IT administrators can be confident that user devices are configured with the correct settings and can be secured in the event of loss, theft or user abuse.



► DETAILED FEATURES OF KASPERSKY SECURITY FOR MOBILE:

IT EFFICIENCY FEATURES:

SIMPLE CONFIGURATION VIA A SINGLE CONSOLE

Unlike other solutions, Kaspersky Lab allows administrators to use only one console to manage the security of mobile devices, physical endpoints, virtual systems, encryption and policy enforcement tools.

PRIVATE APPLICATION PORTAL

Administrators publish a corporate portal that contains links to approved applications. Users can be limited to only these applications.

“OVER THE AIR” PROVISIONING

Secures phones remotely by sending either an email or SMS containing a link to the corporate portal where users can download the profile and applications you've approved. Access to data won't be granted until the user has accepted.

SECURE CONFIGURATION

Ensures hardware and software integrity by enabling rooting and jailbreak detection. Other security settings include 'camera disable', forced password and more.

COMPLIANCE AND POLICY ENFORCEMENT

Application control allows the monitoring and control of application usage on the device including 'Default Deny' and 'Default Allow' support.

SECURITY RISK CONTROL:

ENCRYPTION

Data in motion is protected via transparent full-disk and file level data encryption which can also be applied to a container.

ANTI-THEFT

Administrators can remotely perform a full or selective device wipe, pinpoint the location of a missing device using GPS "Find" and receive notification if a SIM card is removed or swapped.

MOBILE ANTI-MALWARE

Kaspersky Lab's anti-malware engine features multiple layers of detection including cloud-assisted protection, and combines with a safe browser and powerful anti-spam to ensure the device is not compromised by malicious software.

CORPORATE AND PERSONAL DATA INTEGRITY:

CONTAINERS

In support of an employee-owned device scenario, corporate data and applications can be placed in isolated "containers". This provides maximum security for corporate data, and optimal integrity for personal content.

REMOTE DATA SAFETY TOOLS

In the event a device is misplaced, Remote Lock can be engaged. Corporate data within a container on the device can be secured, encrypted, remotely managed and wiped independently of personal data on the device.

How to buy

Kaspersky Mobile Security is included in these users of Kaspersky Endpoint Security for Business:

- Endpoint Security, Select
- Endpoint Security, Advanced
- Kaspersky Total Security for Business

Kaspersky Security for Mobile can also be purchased separately. Contact your reseller for details and pricing.

NOT ALL FEATURES ARE AVAILABLE ON ALL PLATFORMS.
For details, please consult www.kaspersky.com

KESB-MOBILE/Version 0.3/Nov12/Global

Kaspersky Lab ZAO,
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com
usa.kaspersky.com | securelist.com

© 2012 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries. Android is a trademark of Google, Inc. Mac OS is a registered trademark of Apple Inc. The Trademark Blackberry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

