KASPERSKY SECURITY FOR MOBILE

Multilayer security, management and control for all mobile endpoints

Mobile devices are increasingly attractive to cybercriminals. Meanwhile, "bring your own device" (BYOD) is contributing to an increasingly complex mix of devices, creating a challenging management and control environment for IT administrators.

Kaspersky Security for Mobile ensures your device is safe, no matter where it is. Protect against constantly evolving mobile malware. Quickly and easily gain visibility and control over the smartphones and tablets in your environment, from one central location and with minimal disruption.

- Powerful Anti-Malware
- Anti-Phishing and Anti-Spam
- Web protection
- Application Control
- Rooting/jailbreak detection
- Containerization
- Anti-Theft
- Mobile Device Management
- Self-Service Portal
- Centralized management
- Web Console
- Supported platforms:
  - Android™
  - iOS®
  - Windows Phone®

HIGHLIGHTS

ADVANCED ANTI-MALWARE FOR MOBILE DEVICE AND DATA SECURITY

In 2014 alone, Kaspersky Lab dealt with almost 1.4 million unique mobile malware attacks . Kaspersky Security for Mobile combines anti-malware with deep layers of protection technologies, guarding against known and unknown threats to data stored on mobile devices.

MOBILE DEVICE MANAGEMENT (MDM)

Integration with all leading mobile device management platforms enables remote over the air (OTA) deployment and control for easier usability and management of Android, iOS and Windows Phone devices.

MOBILE APPLICATION MANAGEMENT (MAM)

Containerization and selective wipe capabilities enable separation of business and personal data on the same device – supporting BYOD initiatives. Combined with our encryption functionality and anti-malware, this makes Kaspersky Security for Mobile a proactive mobile protection solution, rather than one that simply attempts to isolate a device and its data.

CENTRALIZED MANAGEMENT

Manage multiple platforms and devices from the same console as other endpoints – increase visibility and control without additional effort or technology to manage.

MOBILE SECURITY AND MANAGEMENT FEATURES

POWERFUL ANTI-MALWARE
Signature-based, proactive and cloud-assisted (via Kaspersky Security Network – KSN) protection from known and unknown mobile malware threats. On-demand and scheduled scans combine with automatic updates to increase protection.

ANTI-PHISHING AND ANTI-SPAM
Powerful Anti-Phishing and Anti-Spam technologies protect the device and its data from phishing attacks and help filter out unwanted calls and texts.

WEB CONTROL/SAFE BROWSER
Supported by Kaspersky Security Network (KSN), these technologies work in real time to block access to malicious and unauthorized Web sites. A Safe Browser delivers constantly updated reputation analysis, ensuring safe mobile browsing.

APPLICATION CONTROL
Integrated with KSN, Application Controls restrict application use to approved software only, prohibiting use of grey or unauthorized software. Make device functionality dependent on installation of required applications. Application inactivity control enable admins to require user re-login if an application is idle for a defined period of time. This protects data even if an application is open when the device is lost or stolen.

ROOTING/JAILBREAK DETECTION
Automatic detection and reporting of rooting or jailbreaking can be followed with automatic blocking of access to containers, selective wiping or entire device wipe.

CONTAINERIZATION
Separate business and personal data by "wrapping" applications into containers. Additional policies, such as encryption, can be applied to protect sensitive data. Selective wipe enables the deletion of containerized data on a device when an employee leaves, without impacting his or her personal data.

ANTI-THEFT
Remote Anti-Theft features including wipe, device lock, locate, SIM watch, mugshot and alarm device detection can be activated in the event of device loss or theft. Depending on the case, the anti-theft commands can be applied in a very flexible way. For example, integration with Google Cloud Messaging (GCM) allows delivering the commands almost immediately, increasing reaction times and improving security, while sending commands through the Self-Service Portal doesn't require actions from administrator.

MOBILE DEVICE MANAGEMENT (MDM)
Support for Microsoft® Exchange ActiveSync®, Apple® MDM and Samsung KNOX™ 2.0 – enables a wide range of policies, through a unified interface, regardless of the platform. E.g., enforcing encryption and passwords or controlling camera use, applying policies to individual users or groups, managing APN/VPN settings.

SELF-SERVICE PORTAL
Delegate routine security management to employees, enable self-registration of approved devices. During new device enablement process, all required certificates can be delivered automatically through the portal, no need for administrator involvement. In case of the device loss, the employee can perform all available Anti-Theft actions through the portal.

CENTRALIZED MANAGEMENT
Manage all mobile devices centrally, from a single console, which also allows managing IT security for all other endpoints.

Web Console allows administrators control and manage devices remotely, from any computer.

How to buy

Kaspersky Security for Mobile is included in:
- Kaspersky Endpoint Security for Business – Select
- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

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

Insight

KASPERSKY lab THE POWER OF PROTECTION

© 2016 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.