KASPERSKY MOBILE SECURITY FOR ENTERPRISE

Securing mobile devices beyond your perimeter

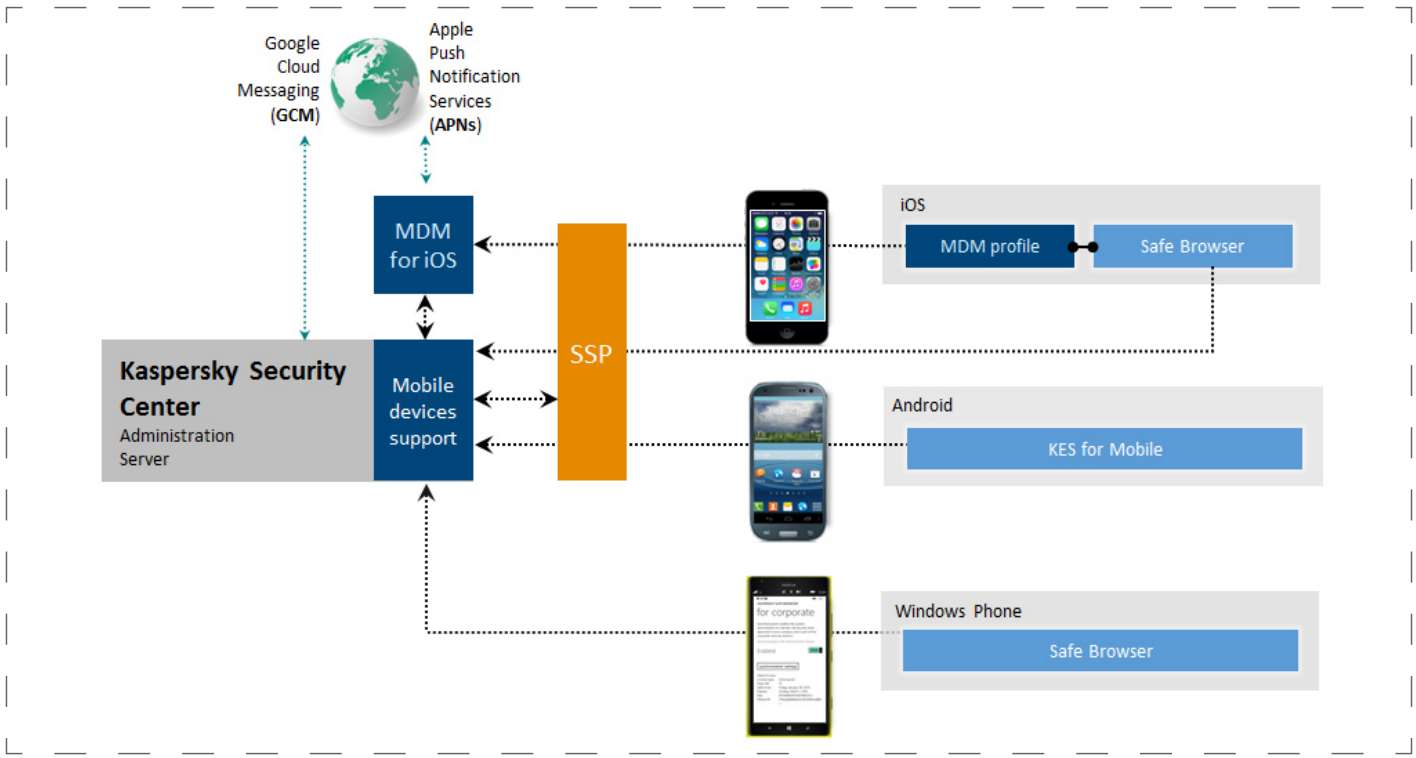
The volume and sophistication of cyberthreats specifically targeting mobile devices is growing exponentially, as cybercriminals recognize the value of the corporate data they can carry. But the threat does not stop there. An under-secured mobile device may prove a convenient conduit deep into your network – with catastrophic long-term consequences in terms of reputational as well as financial damage.

The productivity benefits of 'anytime, anywhere' access to data are too great to be ignored, and BYOD - where employees use their own smartphones and tablets to perform work tasks – continues to grow in popularity. But these developments introduce new elements of risk which must be fully addressed if the organization as a whole is to remain secure. The need for effective mobile security technologies has never been greater.

Kaspersky Security for Mobile protects and controls your corporate data on mobile devices, and secures the devices themselves, covering all major platforms in a single enterprise solution.

Deep levels of threat protection combine with application and web controls to regulate access and usage, while 'app-wrapping' isolates and secures corporate data in wipe-able, encrypted containers on the device. A rich array of anti-theft features, triggered by the user or by IT, allows immediate and decisive action to be taken if any device is mislaid, stolen or under threat.

Mobile Device and Applications Management (MDM/MAM) combines with Kaspersky Lab's outstandingly powerful multi-layered protection into a unified security solution administered from one console – Kaspersky Security Center - together with all your physical and virtual endpoints, or through role-based administration if preferred.



Solution architecture

Key Features

MULTILAYERED 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.

CENTRALIZED OR ROLE-BASED MANAGEMENT

All mobile devices are managed from a single console, together with all other endpoints. Remote management from any computer is through a Web Console. Role-based administration can be implemented if required.

APPLICATION CONTROL

The user can be restricted to safe applications, prohibiting the use of grey or unauthorized software; device functionality can even be dependent on installing specific applications. Inactivity control requires re-login if an application is idle for specified time period, protecting data even if an application is open when the device is lost or stolen.

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. Enforce encryption and passwords or control camera use, applying policies to individual users or groups, managing APN/VPN settings etc

ANTI-PHISHING AND ANTI-SPAM

Powerful Anti-Phishing and Anti-Spam technologies protect the device and its data from phishing.

WEB CONTROL/SAFE BROWSER

Constantly updated reputation analysis in real time is used to block access to malicious and unauthorized web sites, and to ensure safe mobile browsing.

ANTI-THEFT

Remote Anti-Theft features include wipe, device lock, locate, SIM watch, 'mugshot' and 'alarm' device detection. Commands can be applied flexibly; instant messaging with Google Cloud Messaging (GCM) increases reaction times, while using the Self-Service Portal (see below) requires no action from the administrator.

CONTAINERIZATION

Keep business and personal data separate by 'wrapping' applications into containers. Containerized sensitive data can be selectively encrypted or wiped on an employee device, without impacting personal data. For Android devices, applications can also be installed, contained and controlled inside a single wipe-able 'work profile' deployed to the device.

ROOTING/JAILBREAK DETECTION

Automatic detection and reporting can be followed with automatic blocking of container access, or selective wipe or entire device wipe.

SELF-SERVICE PORTAL

Delegate routine security admin tasks, such as the registration of approved devices (including automated certificate generation), to the employee. If a device is lost, the employee can perform all available anti-theft actions directly through the portal.

To learn more about securing your mobile endpoints more effectively, please contact the Kaspersky Lab Enterprise Sales Team.

Kaspersky Mobile Security for Enterprise/Dec 15/Global