Kaspersky®
Mobile Security

Multilayered security, management and control for all mobile endpoints

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 undersecured 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.

Highlights

Advanced Anti-Malware for Mobile Device and Data Security

Mobile malware is increasing exponentially – growing threefold between 2015-16. Ransomware targeting Android-based devices increased four-fold in 2016. Kaspersky Security for Mobile combines anti- malware with cloud-assisted threat intelligence and machine learning to guard against known, unknown and advanced threats to data stored on mobile devices

Mobile Application Management (MAM)

Containerization enables the separation of business and personal data on the same device. Business data stored in protected containers can be encrypted, password protected and further secured against malware. Selective wipe facilitates BYOD.

Mobile Device Management (MDM)

Group policies for Android, iOS and Windows Phone – set up/enable rules for passwords, encryption, Bluetooth and camera. Run reports on the device and applications installed. Integration with all leading mobile device management platforms enables remote 'Over the Air' (OTA) deployment and control for easier usability and management of supported devices.

Centralized Solution Management

Kaspersky Security for Mobile allows you to manage mobile devices from the same console as other endpoint platforms: Kaspersky Security Center or Kaspersky Endpoint Security Cloud. View data on devices, create and manage policies, send commands to devices and run reports – all from one easy-to-manage, central console.

Powerful Anti-Malware

Proactive, cloud-assisted threat detection and analysis combined with traditional technologies to provide protection from known, unknown and advanced threats. On-demand and scheduled scans combine with automatic updates for enhanced 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

Reliable, safe web filtering is supported in real- time by the constantly updated Kaspersky Security Network (KSN) to block access to malicious and other unwanted web sites. Android devices are supported via Chrome-based browsers; for iOS and Windows Phone, Kaspersky Safe Browser is available.

Application Control

Restrict application use to administrator-approved software only. Application control provides data on installed software and enables administrators to enforce installation of specific applications. KSN-integration enables easy creation and management of black and whitelists.

Rooting/Jailbreak Detection

On approximately 5% of mobile devices administrative tasks can be performed on them without user consent or action. Kaspersky Security for Mobile eliminates this risk by detecting rooted or jailbroken devices and alerting administrators, who can block or selectively wipe them.

Application Containerization

Separate business and personal data by 'wrapping' applications into containers, apply additional policies, such as encryption, to protect sensitive data. Selectively wipe containerized data when an employee leaves, without impacting personal data. Enforce authorization for container access – and require additional authorization followed specified period of inactivity.

Anti-Theft

Protect business data, even when devices are stolen, using remote anti-theft features such as device locate-and-lock, selective or full wipe, SIM watch, 'mugshot' and alarm activation. Integration with Google Firebase Cloud Messaging (GCM) and Apple Push Notification Services (APNs) enables near-immediate command delivery. With user self-service portal there is no need to lose time waiting for administrator to activate anti-theft measures.

Mobile Device Management (MDM)

Support for Microsoft® Exchange ActiveSync®, iOS MDM and Samsung KNOX™ enables creation of unified or separate policies for each platform, e.g. mandatory encryption, password enforcement, camera usage, APN/ VPN settings. Android for Work enables business profile creation, business application and device management.

Self-Service Portal

Delegate routine security management to employees, enable self-registration of approved devices. During the new device enablement process, all required certificates can be delivered automatically through the portal. In case of device loss, employees can perform all available anti-theft actions.

Centralized Solution Management

Manage all functionality within Kaspersky Security Center or Kaspersky Endpoint Security Cloud – no need for a separate management tool for mobile devices, simply take care of endpoint and mobile from the same console.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com