Kaspersky®
Mobile Security

Multilayered security, management and control for all mobile endpoints

As mobile devices proliferate, productivity benefits. But the demand for 'anytime anywhere' access to information, which involves your corporate data travelling on personal devices (BYOD) outside your IT perimeter, introduces new elements of risk.

Meanwhile, the volume and sophistication of cyberthreats specifically targeting mobile devices continues to grow, as cybercriminals recognize the value of the data these can carry. And the threat doesn't 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 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

During last 3 years the total number of mobile threats has reached 17M, and number of attacked mobile users increased 4 times. 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.

Enterprise Security Mobility Management

Kaspersky Security for Mobile also provides the security-oriented mobile device management (MDM) feature set covering areas like device unlock, encryption status and network access. Flexible device enrollment supports the easier use and management of Android and iOS devices.

Support for 3rd party EMM solutions

Your existing EMM solution can be used to deploy and configure Kaspersky Endpoint Security for Android, straightforwardly aligning your security with current business processes.

Centralized Solution Management

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

Features

Powerful Anti-Malware

Proactive, cloud-assisted threat detection and analysis work 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), blocking access to malicious and other unwanted websites. Android devices are supported via Chrome-based browsers and Samsung Internet Browser; for iOS, 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 the installation of specific applications. KSN Integration enables the easy creation and management of black and whitelists.

Rooting/Jailbreak Detection

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

3rd Party EMM Integration

If your organization has already chosen an EMM solution for device configuration, you may still need to secure files and applications from malware, and to protect your users from phishing and personal data theft. Integration with third party EMMs means you can deploy Kaspersky Endpoint Security for Android, and enable the management of your security configuration, through your EMM console.

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. Users can activate anti-theft measures directly through the self-service portal.

Mobile Device Management (MDM)

Support for Microsoft® Exchange ActiveSync®, iOS MDM and Samsung KNOX™ enables the creation of unified or separate policies for each platform, covering areas like mandatory encryption, password enforcement, camera use restriction or APN/ VPN settings. Kaspersky Security for Mobile enables the secure creation of an Android Enterprise business profile, allowing us to work with your chosen settings and applications.

Self-Service Portal

Delegate routine security management and enable the self-registration of approved devices. During the new device enablement process, all required certificates can be delivered automatically through the portal. If a device is lost, employees can perform all available anti-theft actions themselves, .so critical time is not lost or valuable resources wasted by having to involve an administrator.

Centralized Solution Management

Manage security functionality for all your mobile platforms. as well as your physical and virtual desktops and servers. through Kaspersky Security Center. No need for separate consoles.

Expert analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence