KASPERSKY SECURITY FOR MOBILE

Bessere Verwaltung und Sicherheit für mobile Endpoints, ohne die Komplexität einer separaten Lösung.

Die Bereitstellung, Verwaltung und Sicherung Ihrer mobilen IT-Umgebung muss weder kompliziert noch teuer sein. **Durch die Verwaltung mobiler Geräte ist die sichere Konfiguration von Mobilgeräten einfach und unkompliziert.** Ein mobiler Agent wird auf dem Gerät installiert, um den Schutz bereitzustellen, den Sie vor heutigen Bedrohungen benötigen, und das sogar auf mitarbeitereigenen Geräten!

Hauptfunktionen:

- SUPPORT FÜR TABLETS UND SMARTPHONES
- „OVER THE AIR"-BEREITSTELLUNG (OTA)
- BEWÄHRTE, AGENTENBASIERTE MOBILE SICHERHEIT
- SICHERE IMPLEMENTIERUNG VON APPLE MDM UND MICROSOFT EXCHANGE ACTIVESYNC
- SYSTEMEIGENE INTEGRATION MIT KASPERSKY SECURITY CENTER FÜR KONFIGURATION, STEUERUNG, BERICHTERSTATTUNG, BESTANDSAUFNAHME UND RICHTLINIENEINSTELLUNG

Unterstützte Mobilplattformen:

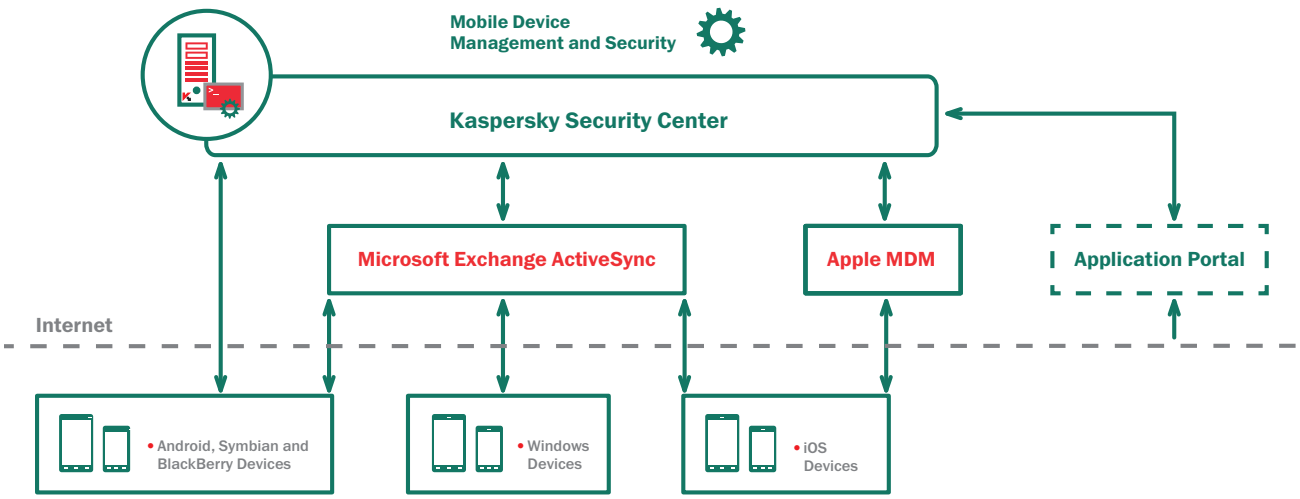
- iOS
- ANDROID™
- WINDOWS® PHONE
- WINDOWS MOBILE
- BLACKBERRY®
- SYMBIAN

PERFEKT FÜR BYOD-INITIATIVEN („BRING YOUR OWN DEVICE")

Viele Mitarbeiter nutzen ihre eigenen Geräte für persönliche wie auch für geschäftliche Aufgaben. Manche Unternehmen ermutigen ihre Mitarbeiter sogar, ihr bevorzugtes Smartphone oder Tablet selbst zu kaufen. Die IT-Abteilung fügt dann den E-Mail- und Unternehmenszugang zum mitarbeitereigenen Gerät hinzu.

Dadurch lassen sich Einsparungen und Produktivitätssteigerungen erzielen, doch die Nutzung mitarbeitereigener Geräte kann für das Unternehmen auch ein Sicherheitsrisiko bedeuten. Unternehmensdaten, die nicht korrekt gesichert und möglicherweise zusammen mit persönlichen Elementen vermischt sind, können leicht abhanden kommen oder in unbefugte Hände geraten. Diese Geräte werden häufig ohne Rücksicht auf Anwendungssicherheit von Familienmitgliedern genutzt. Manche werden sogar gerootet oder einem Jailbreak unterzogen.

Kaspersky Security for Mobile löst diese Probleme durch die Aktivierung der sicheren Konfiguration und Bereitstellung von Smartphones und Tablets über die gleiche Konsole, die auch für Ihre Netzwerksicherheit verwendet wird. IT-Administratoren können sich darauf verlassen, dass Benutzergeräte mit den korrekten Einstellungen konfiguriert sind und bei Verlust, Diebstahl oder Benutzermissbrauch abgesichert werden können.



DETAILLIERTE FUNKTIONEN VON KASPERSKY SECURITY FOR MOBILE:

MERKMALE DER IT-EFFIZIENZ:

EINFACHE KONFIGURATION ÜBER EINE KONSOLE
Im Gegensatz zu anderen Lösungen brauchen Administratoren mit Kaspersky Lab nur eine Konsole zu verwenden, um die Sicherheit von mobilen Geräten, physischen Endpoints, virtuellen Systemen, Verschlüsselung und Tools zur Richtliniendurchsetzung zu verwalten.

PRIVATES ANWENDUNGSPORTAL
Administratoren veröffentlichen ein Unternehmensportal mit Links zu genehmigten Anwendungen. Die Benutzer können auf diese Anwendungen beschränkt werden.

„OVER THE AIR“ PROVISIONING
Sichern Sie Telefone aus der Ferne, indem Sie entweder eine E-Mail oder eine SMS mit einem Link zum Unternehmensportal senden, von dem Benutzer das Profil und von Ihnen genehmigte Anwendungen herunterladen können. Der Zugriff auf Daten wird erst dann gestattet, wenn der Benutzer die Bedingungen akzeptiert hat.

SICHERE KONFIGURATION
Stellen Sie die Hardware- und Softwareintegrität sicher, indem Sie die Erkennung von Rooting und Jailbreaks aktivieren. Weitere Sicherheitseinstellungen sind „Camera disable“, Kennwort erzwingen u. a.

EINHALTUNG UND RICHTLINIENDURCHSETZUNG
Über die Komponente Programmkontrolle können Sie die Anwendungsnutzung auf dem Gerät überwachen und steuern, einschließlich der Unterstützung für die Richtlinien „Default Deny“ und „Default Allow“.

SICHERHEITSRISIKOSTEUERUNG:

VERSCHLÜSSELUNG
Übertragene Daten werden durch eine transparente Datenverschlüsselung für den gesamten Datenträger oder auf Dateiebene, geschützt, die auch auf einen Container angewendet werden kann.

DIEBSTAHLSCHUTZ
Administratoren können aus der Ferne eine vollständige oder selektive Gerätelöschung durchführen, den Standort eines vermissten Geräts mithilfe von GPS bestimmen und eine Benachrichtigung erhalten, wenn eine SIM-Karte entfernt oder ausgetauscht wird.

MOBILE ANTI-MALWARE
Die Anti-Malware-Engine von Kaspersky Lab weist mehrere Erkennungsebenen auf, einschließlich Cloud-basierten Schutz, und kombiniert einen sicheren Browser, um sicherzustellen, dass das Gerät nicht durch gefährliche Software manipuliert wird.

UNTERNEHMENS- UND PERSÖNLICHE DATENINTEGRITÄT:

CONTAINER
Zur Unterstützung von mitarbeitereigenen Geräten können Unternehmensdaten und -anwendungen in isolierten „Containern“ platziert werden. Dadurch wird maximale Sicherheit für die Unternehmensdaten und optimale Integrität für persönliche Inhalte gewährleistet.

TOOLS FÜR DIE SICHERHEIT VON REMOTE-DATEN
Wenn ein Gerät verloren gegangen ist, kann die Remote-Sperre aktiviert werden. Die Unternehmensdaten in einem Container auf dem Gerät können unabhängig von den persönlichen Daten auf dem Gerät gesichert, verschlüsselt, aus der Ferne verwaltet und gelöscht werden.

How to buy

Kaspersky Mobile Security ist in folgenden Versionen von **Kaspersky Endpoint Security for Business** enthalten:

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

Kaspersky Security for Mobile kann auch separat erworben werden. Setzen Sie sich für Informationen und Preise mit Ihrem Vertriebspartner in Verbindung.

MANCHE FUNKTIONEN WERDEN VON BESTIMMTEN PLATTFORMEN NICHT UNTERSTÜTZT. Nähere Informationen erhalten Sie unter **www.kaspersky.de.**

Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | salesdach@kaspersky.de

gwmsa/Stand: Januar 2013