▶ KASPERSKY SECURITY FOR MOBILE

Mehrstufiger Schutz, Management und Kontrolle für alle mobilen Endpoints

Mobile Geräte werden auch für Cyberkriminelle immer interessanter. Beruflich genutzte Mobilgeräte von Mitarbeitern (BYOD) sind der Grund für einen immer komplexer werdenden Gerätemix und schaffen eine höchst anspruchsvolle Management- und Kontrollsituation für IT-Administratoren.
Mit Kaspersky Security for Mobile haben Sie die Gewissheit, dass Ihr Gerät gut geschützt ist, egal wo es sich gerade befindet. Sorgen Sie für Schutz vor sich ständig weiterentwickelnder Malware. Sehen Sie auf einen Blick alle Smartphones und Tablets in Ihrem Netzwerk - von einer Konsole aus.

- **Leistungsstarker Malware-Schutz**
- **Phishing- und Spam-Schutz**
- **Web-Schutz**
- **Programmkontrolle**
- **Erkennung von „Rooting“ und „Jailbreak“**
- **Containerisierung**
- **Diebstahlschutz**
- **Mobile Device Management**
- **Self-Service-Portal**
- **Zentralisierte Verwaltung**
- **Web Console**
- **Unterstützte Plattformen:**
  - Android™
  - iOS
  - Windows Phone

WICHTIGSTE VORTEILE

WEGWEISENDER MALWARE-SCHUTZ FÜR MOBILGERÄTE UND DATEN

Allein im Jahr 2014 haben wir bei Kaspersky Lab fast 1,4 Millionen singuläre Attacken durch mobile Malware erfasst. Kaspersky Security for Mobile kombiniert Malware-Schutz mit tiefgreifender Sicherheit, die Daten auf mobilen Geräten vor bekannten und unbekannten Bedrohungen schützt.

MOBILE DEVICE MANAGEMENT (MDM)

Integration mit allen führenden Mobile-Device-Management-Plattformen ermöglicht OTA (Over The Air)-Bereitstellungen und OTA-Kontrolle per Fernzugriff und erleichtert Bedienbarkeit und Verwaltung von Android-, iOS- und Windows Phone-Geräten.

MOBILE APPLICATION MANAGEMENT (MAM)

Containerisierung und selektive Löschung ermöglichen die Trennung von geschäftlichen und privaten Daten auf ein und demselben Gerät und unterstützen auf diese Weise Ihre BYOD-Initiativen. Im Zusammenspiel mit unseren Verschlüsselungs- und Malware-Schutzfunktionen wird aus Kaspersky Security for Mobile eine proaktive Lösung zum Schutz von Mobilgeräten – im Gegensatz zu anderen Ansätzen, die Geräte und Daten einfach nur isolieren.

ZENTRALES MANAGEMENT

Verwalten Sie eine Vielzahl von Plattformen und Geräten von derselben Konsole aus, über die auch andere Endpoints verwaltet werden, und steigern Sie Transparenz und Kontrolle ohne erhöhten Aufwand oder zusätzliche Technologien.

SICHERHEIT UND VERWALTUNG MOBILER GERÄTE – FUNKTIONEN

LEISTUNGSSTARKER MALWARE-SCHUTZ
Proaktiver, Signatur- und cloudbasiert Schutz (über das Kaspersky Security Network, KSN) vor bekannten und unbekannten Bedrohungen durch mobile Malware. Bedarfsabhängige oder zeitplangesteuerte Scans und automatische Updates sorgen für noch mehr Schutz.

PHISHING- UND SPAM-SCHUTZ
Leistungsstarke Technologien für Phishing- und Spam-Schutz schützen Geräte und Daten und ermöglichen die Blockierung unerwünschter Anrufe und SMS-Nachrichten.

WEB-KONTROLLE/FUNKTION „SICHERER BROWSER“
Auf Grundlage von Echtzeitdaten aus dem Kaspersky Security Network (KSN) blockieren diese Technologien den Zugriff auf schädliche und nicht-autorisierte Webseiten. Die Funktion „Sicherer Browser“ bietet eine stets aktuelle Reputationsanalyse und sorgt für eine sichere Internetnutzung auf mobilen Geräten.

PROGRAMMKONTROLLE
Die mit KSN integrierten Programmkontrollen beschränken die Programmnutzung auf genehmigte Programme und verhindern die Verwendung unsicherer oder nicht genehmigter Software. Machen Sie die Funktionalität des Geräts von den dort installierten Programmen abhängig. Durch die Überwachung des Inaktivitätszeitraums von Programmen kann eine erneute Anmeldung durch den Benutzer erzwungen werden, falls für einen vorgegebenen Zeitraum keine Benutzereingabe erfolgt ist. Auf diese Weise sind die Daten geschützt, selbst wenn ein Programm geöffnet ist und das Gerät abhanden kommt oder gestohlen wird.

ERKENNUNG VON „ROOTING“ UND „JAILBREAK“
Die automatische Erkennung von „Rooting“- und „Jailbreak“-Versuchen lässt sich mit einer automatischen Zugriffssperre für Container bzw. einer selektiven oder vollständigen Löschung der Gerätedaten kombinieren.

Hinweise zum Kauf

Kaspersky Security for Mobile ist Teil von:

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

Kaspersky Security for Mobile ist auch separat als Targeted Solution erhältlich.

Setzen Sie sich mit Ihrem Vertriebspartner in Verbindung, um Informationen und Preise zu erhalten.

CONTAINERISIERUNG
Trennung von geschäftlichen und persönlichen Daten durch Kapselung von Programmen in Containern. Zum Schutz vertraulicher Daten können zusätzliche Richtlinien angewendet werden, z. B. für die Verschlüsselung. Durch selektives Löschen können die Containerdaten auf einem Gerät gezielt gelöscht werden, ohne dabei die persönlichen Daten des Mitarbeiters zu beeinträchtigen.

DIEBSTAHLSCHUTZ
Per Fernzugriff steuerbare Diebstahlschutz-Funktionen wie Löschen, Gerätesperre, Ortung, SIM-Kontrolle, Fahndungsfoto und Alarm können bei Verlust oder Diebstahl des Geräts ausgelöst werden. Die Diebstahlschutz-Befehle können äußerst flexibel eingesetzt werden. Durch die Integration mit Google Cloud Messaging (GCM) können die Funktionen beispielsweise fast umgehend genutzt werden, was zu verkürzten Reaktionszeiten und gesteigerter Sicherheit führt, während die Verwendung des Self-Service-Portals zur Bedienung der Diebstahlschutz-Funktionen den Administrator entlastet.

MOBILE DEVICE MANAGEMENT (MDM)
Unterstützung von Microsoft Exchange ActiveSync, Apple MDM und Samsung KNOX 2.0 ermöglicht die Nutzung unterschiedlichster Richtlinien über eine einzige, plattformunabhängige Benutzeroberfläche. Durchsetzen von Verschlüsselung und Kennwörtern oder Steuerung der Kamerafunktion, Richtlinienanwendung für einzelne Benutzer oder Benutzergruppen, Verwalten von APN/VPN-Einstellungen, um nur einige Beispiele zu nennen.

SELF-SERVICE-PORTAL
Überlassen Sie routinemäßige Sicherheitsabläufe Ihren Mitarbeitern, und ermöglichen Sie eine selbstständige Anmeldung von genehmigten Geräten. Während der Aktivierung neuer Geräte können alle erforderlichen Zertifikate ohne Beteiligung des Administrators automatisch über das Portal bereitgestellt werden. Im Fall eines Geräteverlusts kann der Eigentümer alle verfügbaren Diebstahlschutz-Funktionen über das Portal aktivieren.

ZENTRALES MANAGEMENT
Zentrale Verwaltung aller Mobilgeräte von einer einzigen Konsole aus, über die auch die Sicherheit aller anderen Endpoints kontrolliert wird. Unsere Webkonsole gibt Ihren Administratoren die Möglichkeit, Geräte per Fernzugriff von jedem beliebigen Computer aus zu kontrollieren und zu verwalten.

Kaspersky Security for Mobile/Feb 15/Global

KASPERSKY lab