Kaspersky Security for Mobile

Mehrstufiger Schutz, Verwaltung und Kontrolle für alle mobilen Endpoints

Funktionen

Leistungsstarker Malware-Schutz
Phishing- und Spam-Schutz
Web-Schutz
Programmkontrolle
Erkennung von „Rooting" und „Jailbreak"
Mobile Application Management
Diebstahlschutz
Mobile Device Management
Self-Service-Portal
Zentrale Lösungsverwaltung
Webkonsole

Unterstützte Plattformen:

- Android™
- iOS
- Windows 10 Mobile

Nutzen Sie die Vorteile mobiler Endgeräte. Aber sicher!

Kaspersky Security for Mobile ist eine Lösung zur Abwehr von Bedrohungen auf Mobilgeräten (MTD, Mobile Threat Defense und MTM, Mobile Threat Management), die Unternehmen bei der Steigerung der Produktivität und Effizienz hilft, indem Mitarbeiter Aufgaben auch unterwegs sicher durchführen können – egal, wo sie sich befinden.

2016 entdeckte Kaspersky Lab fast 8,5 Milliarden Angriffe auf Mobilgeräte durch Malware. Mitarbeiter haben durchschnittlich drei mobile Geräte. Sicherheit ist also ein zentrales Thema. Kaspersky Security for Mobile bietet hohe mobile Sicherheit mit minimalem Aufwand.

Wichtigste Vorteile

VERBESSERTER MALWARE-SCHUTZ

Die Menge mobiler Malware steigt weiter an. Allein im ersten Halbjahr 2017 überschritt die Anzahl an mobilen Ransomware-Bedrohungen die Anzahl der im gesamten Jahr 2016 erkannten Bedrohungen. Auf Android-basierte Geräte abgezielte Ransomware hat im Jahr 2016 um das Vierfache zugenommen.

Kaspersky Security for Mobile vereint Malware-Schutz mit Cloud-basierter Threat Intelligence und lernfähigen Systemen, und schützt mobile Geräte so vor bekannten, unbekannten und hoch entwickelten Bedrohungen zu schützen.

MOBILE DEVICE MANAGEMENT (MDM)

Gruppenrichtlinien für Android, iOS und Windows 10 Mobile – Definieren/Aktivieren Sie Regeln für Passwörter, Verschlüsselung, Bluetooth und Kamera. Sie können Berichte zum Gerät und den installierten Anwendungen ausführen. Die Integration in alle führenden Mobile-Device-Management-Plattformen ermöglicht eine OTA-Bereitstellung (Over The Air) und -Kontrolle per Fernzugriff, sodass unterstützte Geräte einfacher bedient und verwaltet werden können.

MOBILE APPLICATION MANAGEMENT (MAM)

Mit der Programmkontrolle für Android und iOS können Nutzer festlegen, welche Apps installiert werden dürfen und Blacklists und Whitelists für diese Apps erstellen.

FLEXIBLE EINSATZOPTIONEN

Flexible Abonnementoptionen unterstützen sowohl BYOD und COPE-Szenarien (Company-Owned, Personally Enabled). Einsätze in einer BYOD-Umgebung können ganz einfach über Google Play oder dem App Store installiert werden. Diejenigen mit einer COPE-Strategie können dies über das Self-Service-Portal oder eine benutzerdefinierte Installation tun. So bleiben Unternehmen flexibel und können ihre Sicherheitsstrategie beibehalten.

ZENTRALE LÖSUNGSVERWALTUNG

Mit Kaspersky Security for Mobile können Sie mobile Geräte über dieselbe Konsole wie andere Endpoint-Plattformen verwalten: Kaspersky Security Center oder Kaspersky Endpoint Security Cloud. Sie können Daten auf Geräten anzeigen, Richtlinien erstellen und verwalten, Befehle an Geräte senden und Berichte ausführen – all das über eine benutzerfreundliche und zentrale Konsole.

Sicherheit und Verwaltung mobiler Geräte – Funktionen

LEISTUNSSTARKER MALWARE-SCHUTZ
Die reaktionsschnelle, Cloud-basierte Erkennung und Analyse von Bedrohungen bieten in Kombination mit herkömmlichen Technologien Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen. Bedarfsabhängige oder zeitplangesteuerte Scans und automatische Updates sorgen für einen erweiterten Schutz.

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

WEB-KONTROLLE/FUNKTION „SICHERER BROWSER"
Die zuverlässige und sichere Webfilterung wird in Echtzeit von dem regelmäßig aktualisierten Kaspersky Security Network (KSN) unterstützt und blockiert den Zugriff auf schädliche und andere unerwünschte Websites. Android-Geräte werden über Chrome-basierte Browser unterstützt. Für iOS und Windows 10 Mobile steht die Kaspersky-Funktion „Sicherer Browser" zur Verfügung.

PROGRAMMKONTROLLE
Schränken Sie die Nutzung von Programmen auf vom Administrator genehmigte Software ein. Die Programmkontrolle stellt Daten auf installierter Software bereit und ermöglicht Administratoren das Erzwingen der Installation bestimmter Anwendungen. Die KSN-Integration ermöglicht eine einfache Erstellung und Verwaltung von Blacklists und Whitelists.

ERKENNUNG VON „ROOTING" UND „JAILBREAK"
Auf rund 5 % der mobilen Geräte können Verwaltungsaufgaben ohne Benutzerzustimmung oder -aktion ausgeführt werden. Kaspersky Security for Mobile verhindert dieses Risiko durch die Erkennung von Geräten mit Rooting oder Jailbreak und gibt eine Warnung an Administratoren aus, die diese blockieren oder selektiv löschen können.

CONTAINERISIERUNG VON PROGRAMMEN
Sie können Geschäfts- und persönliche Daten durch eine „Kapselung" von Anwendungen in Containern trennen und zusätzliche Richtlinien wie die Verschlüsselung anwenden, um vertrauliche Daten zu schützen. Sie können in Containern gespeicherte Daten selektiv löschen, wenn ein Mitarbeiter das Unternehmen verlässt, ohne persönliche Daten zu beeinträchtigen. Nutzen Sie Autorisierungen für Container-Zugriffe.

DIEBSTAHLSCHUTZ
Schützen Sie Geschäftsdaten auch auf gestohlenen Geräten mithilfe von Anti-Theft-Funktionen wie Geräteortung und -sperre, gezieltes oder vollständiges Löschen, SIM-Kontrolle, „Fahndungsfoto" und Alarmaktivierung. Die Integration in Google Firebase Cloud Messaging (FCM) und Apple Push Notification Services (APNs) ermöglicht eine nahezu sofortige Befehlsbereitstellung. Dank des Self-Service-Portals für Benutzer müssen Sie nicht warten, bis ein Administrator Anti-Theft-Maßnahmen aktiviert.

MOBILE DEVICE MANAGEMENT (MDM)
Die Unterstützung für Microsoft® Exchange ActiveSync®, Samsung KNOX™ und iOS MDM ermöglicht die Erstellung einheitlicher oder separater Richtlinien für jede Plattform, darunter obligatorische Verschlüsselung, Erzwingung von Passwörtern, Nutzung der Kamera, APN-/VPN-Einstellungen. Kaspersky Security for Mobile umfasst darüber hinaus die Verwaltung von iOS-Geräten, sodass Systemadministratoren umfassende Verwaltungsrechte haben und so die Sicherheit erhöht wird. Android for Work ermöglicht die Erstellung von Unternehmensprofilen, Unternehmensanwendungen und Geräteverwaltung sowie die Trennung von geschäftlichen und privaten Daten auf demselben Gerät.

SELF-SERVICE-PORTAL
Überlassen Sie routinemäßige Sicherheitsabläufe Ihren Mitarbeitern, und ermöglichen Sie eine eigenhändige Anmeldung von genehmigten Geräten. Während der Aktivierung der neuen Geräte können alle erforderlichen VPN- und E-Mail-Zertifikate automatisch über das Portal bereitgestellt werden. Bei einem Geräteverlust können Mitarbeiter alle verfügbaren Anti-Theft-Aktionen durchführen.

ZENTRALE LÖSUNGSVERWALTUNG
Verwalten Sie alle Funktionen im Kaspersky Security Center oder in der Kaspersky Endpoint Security Cloud – Sie benötigen kein separates Verwaltungstool für mobile Geräte, sondern verwalten Endpoint- und mobile Geräte einfach über dieselbe Konsole.

Hinweise zum Kauf
- Kaspersky Security for Mobile ist Teil von:
- Kaspersky Endpoint Security Cloud
- 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.

www.kaspersky.de
#truecybersecurity