KASPERSKY MOBILE SECURITY FOR ENTERPRISE

Sicherheit für Mobilgeräte jenseits Ihres Perimeters

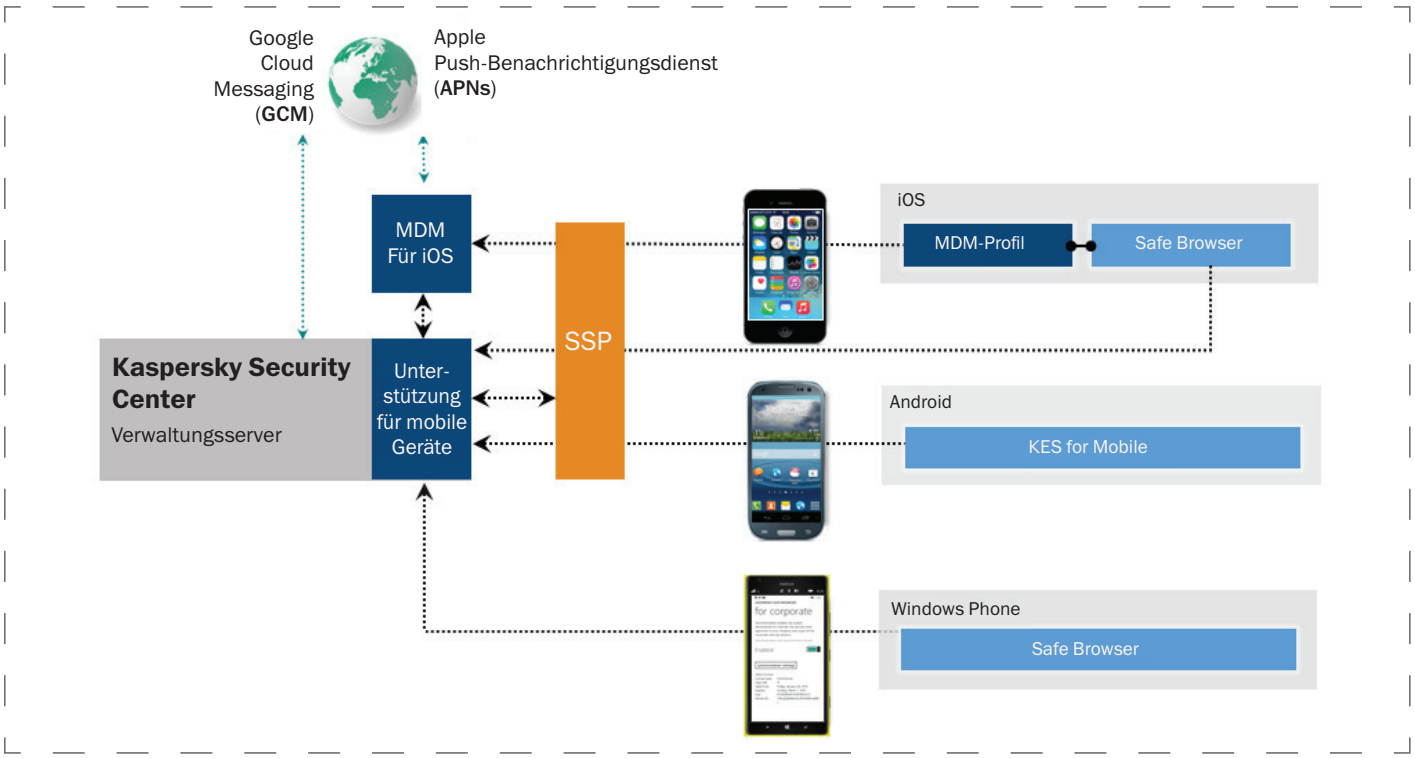
Die Anzahl und die Raffinesse von Cyberbedrohungen, die sich speziell an Mobilgeräte richten, wachsen exponentiell, seit Cyberkriminelle den Wert der Unternehmensdaten, die oftmals auf diesen Geräten gespeichert sind, erkannt haben. Die Bedrohung hört hier jedoch nicht auf. Unzureichend geschützte Mobilgeräte können einen bequemen Weg tief in Ihr Netzwerk darstellen. Mit katastrophalen Folgen langfristigen, rufschädigenden und teuren Folgen für Ihr Unternehmen.

Für die Produktivität der Mitarbeiter ist es von großem Vorteil, wenn sie zu jeder Zeit und von jedem Ort auf Unternehmensdaten zugreifen können. Das sogenannte BYOD, bei dem die Mitarbeiter ihre eigenen Smartphones und Tablets für Arbeitsaufgaben verwenden, gewinnt immer mehr an Popularität. Diese Entwicklungen führen jedoch zu neuen Risiken, die sorgfältig geprüft werden müssen, wenn das Unternehmen als Ganzes geschützt bleiben möchte. Der Bedarf an effizienten Technologien für mobile Sicherheit war nie größer.

Kaspersky Security for Mobile schützt und kontrolliert Ihre Unternehmensdaten auf mobilen Geräten sowie die Geräte selbst mit einer einzigen Unternehmenslösung, die alle großen Plattformen abdeckt.

Der tiefgreifende Schutz vor Bedrohungen sorgt in Kombination mit der Programm- und Web-Kontrolle für die Regulierung von Zugriff und Nutzung, während mithilfe der „Containerisierung" der Anwendungen Unternehmensdaten auf den Geräten in verschlüsselten und vollständig löschbaren Containern isoliert und gesichert werden. Eine große Bandbreite an Diebstahlschutz-Funktionen, die vom Benutzer selbst oder durch die IT ausgelöst werden können, ermöglicht bei Verlust, Diebstahl oder aktueller Bedrohung von Geräten sofortiges Handeln.

Mobile Device Management und Applications Management (MDM/MAM) sorgen in Kombination mit der außerordentlich leistungsstarken mehrstufigen Sicherheitslösung von Kaspersky Lab für eine einheitliche Sicherheitslösung, die über eine Konsole – das Kaspersky Security Center – verwaltet werden kann. Diese Konsole können Sie entweder über Ihre physischen oder virtualisierten Endpoints oder, falls gewünscht, über eine rollenbasierte Administration bedienen.



Die Architektur der Lösung

Hauptfunktionen

MEHRSTUFIGER VIRENSCHUTZ
Schneller Signatur- und Cloud-basierter 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.

PROGRAMMKONTROLLE
Beschränken Sie den Benutzer auf die Verwendung von sicheren Anwendungen oder verbieten Sie die Nutzung von unsicherer und nicht genehmigter Software. Gerätefunktionen können sogar von der Installation von bestimmten Anwendungen abhängig gemacht werden. Die Inaktivitätskontrolle erfordert die erneute Anmeldung, wenn eine Anwendung für einen bestimmten Zeitraum inaktiv war, wodurch die Daten geschützt sind, auch wenn die Anwendung bei Diebstahl oder Verlust des Geräts geöffnet sein sollte.

PHISHING- UND SPAM-SCHUTZ
Leistungsstarke Technologien für Phishing- und Spam-Schutz schützen Geräte und Daten vor Phishing-Angriffen.

DIEBSTAHLSCHUTZ
Zu den per Fernzugriff steuerbaren Diebstahlschutz-Funktionen gehören Löschen, Gerätesperre, Ortung, SIM-Kontrolle, „Fahndungsfoto" und Alarm. Die Befehle können flexibel angewendet werden; das Instant Messaging mit Google Cloud Messaging (GCM) erhöht die Reaktionszeiten, und die Nutzung des Self-Service-Portals (siehe unten) durch den Benutzer erfordert vom Administrator keine weitere Aktion.

ERKENNUNG VON „ROOTING" UND „JAILBREAK"
Die automatische Erkennung und die Berichterstellung lassen sich mit einer automatischen Zugriffssperre für Container oder einer selektiven oder vollständigen Löschung der Gerätedaten kombinieren.

ZENTRALES ODER ROLLENBASIERTES MANAGEMENT
Alle Mobilgeräte werden über eine einzige Konsole gemeinsam mit allen anderen Endpoints verwaltet. Das Remote-Management ist von jedem Computer aus über eine Web-Konsole möglich. Die rollenbasierte Verwaltung kann wie erforderlich implementiert werden.

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.

WEB-KONTROLLE/FUNKTION „SICHERER BROWSER"
Die kontinuierlich aktualisierte Reputationsanalyse in Echtzeit wird verwendet, um Zugriff auf schädliche und nicht autorisierte Webseiten zu blockieren und so ein sicheres Surfen im mobilen Internet zu ermöglichen.

CONTAINERISIERUNG
Trennung von geschäftlichen und persönlichen Daten durch Kapselung von Programmen in Containern. Eingekapselte vertrauliche Daten können auf einem Mitarbeitergerät separat verschlüsselt und gelöscht werden, ohne dass dies die persönlichen Daten beeinträchtigt. Auf Android-Geräten können die Programme auch innerhalb eines einzigen löschbaren „Arbeitsprofils", das auf dem Gerät eingerichtet ist, installiert, isoliert und kontrolliert werden.

SELF-SERVICE-PORTAL
Delegieren Sie routinemäßige Sicherheitsaufgaben des Administrators, wie die Registrierung von zugelassenen Geräten (einschließlich der automatisierten Zertifikatsgenerierung), an den Mitarbeiter. Wenn ein Gerät verloren wird, kann der Mitarbeiter alle verfügbaren Diebstahlschutzmaßnahmen direkt über das Portal durchführen.

Kontaktieren Sie das Kaspersky Lab Enterprise Sales Team, um mehr über die effektive Sicherung Ihrer mobilen Endpoints zu erfahren.

Kaspersky Mobile Security for Enterprise/Dez 15/Global