# 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 Phone

Nutzen Sie die geschäftlichen Vorteile mobiler Geräte ohne Sicherheitseinbußen.

Kaspersky Security for Mobile unterstützt Unternehmen dabei, die Produktivität und Effizienz zu steigern, indem Mitarbeiter Aufgaben auch unterwegs sicher durchführen können.

Alle 40 Sekunden wird ein Unternehmen Opfer eines Cyberangriffs. Allein im dritten Quartal 2016 entdeckte Kaspersky Lab mehr als 1,5 Millionen schädliche mobile Installationspakete. Mit durchschnittlich drei mobilen Geräten pro Mitarbeiter müssen Unternehmen unbedingt sicherstellen, dass diese Geräte sicher sind, wo immer sie sich auch befinden. Kaspersky Security for Mobile bietet hohe mobile Sicherheit mit minimalem Aufwand.

## Wichtigste Vorteile

### WEGWEISENDER MALWARE-SCHUTZ FÜR MOBILGERÄTE UND DATEN

Mobile Malware verbreitet sich exponentiell – mit einem dreifachen Wachstum zwischen 2015 und 2016. Auf Android-basierte Geräte abgezielte Ransomware hat im Jahr 2016 um das Vierfache zugenommen. Kaspersky Security for Mobile vereint Malware-Schutz mit Cloud-basierten Bedrohungsinformationen und lernfähigen Systemen, um auf mobilen Geräten gespeicherte Daten vor bekannten, unbekannten und hoch entwickelten Bedrohungen zu schützen.

### MOBILE DEVICE MANAGEMENT (MDM)

Gruppenrichtlinien für Android, iOS und Windows Phone definieren/aktivieren Regeln für Kennwörter, 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)

Die Containerisierung ermöglicht eine Trennung von Geschäfts- und persönlichen Daten auf demselben Gerät. In geschützten Containern gespeicherte Geschäftsdaten können durch Verschlüsselung, Kennwörter und weitere Sicherheitsmaßnahmen vor Malware geschützt werden. Das gezielte Löschen unterstützt BYOD-Initiativen.

### 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 Phone steht die Kaspersky-Funktion „Sicherer Browser“ zur Verfügung.

**PROGRAMMKONTROLLE**
Schränken Sie die Anwendungsnutzung auf vom Administrator genehmigte Software ein. Die Programmkontrolle stellt Daten auf installierter Software bereit und ermöglicht Administratoren die Erzwingung 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. Erzwingen Sie eine Autorisierung für den Zugriff auf Container, und fordern Sie eine zusätzliche Autorisierung nach einer bestimmten Dauer der Inaktivität ein.

**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 (GCM) 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®, iOS MDM und Samsung KNOX™ ermöglicht die Erstellung einheitlicher oder separater Richtlinien für jede Plattform, darunter obligatorische Verschlüsselung, Erzwingung von Kennwörtern, Nutzung der Kamera, APN-/VPN-Einstellungen. Android for Work ermöglicht die Erstellung von Unternehmensprofilen sowie die Verwaltung von Unternehmensanwendungen und -geräten.

**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 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 for Business 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**