kaspersky BRING ON THE FUTURE

Einheitlicher Endpoint-Schutz von Kaspersky – Mobile Device Security

Damit Unternehmen sicherstellen können, dass ihre Mitarbeiter durch die Nutzung mobiler Geräte keine sensiblen Unternehmensdaten und kritischen Geschäftsprozesse gefährden, bietet Kaspersky eine kombinierte Version der Module Mobile Threat Defense (MTD) und Mobile Threat Management (MTM) an. Darin werden branchenführender Malware- und Spam-Schutz sowie Web-, Programm- und Gerätekontrollen für Android- und iOS-Geräte miteinander kombiniert und um eine Diebstahlsicherungsfunktion ergänzt.

Weiter unten finden Sie eine Liste der einzelnen Mobile Device Security- und Verwaltungsfunktionen.

Mobile Bedrohungen entwickeln sich weiter

Im Laufe der Zeit hat Kaspersky insgesamt mehr als **40 Millionen Bedrohungen gegen Mobilgeräte** identifiziert.

Unsere Umfrage im Jahr 2019 unter Unternehmen weltweit ergab:

- Mehr als **40 %** der Befragten gaben an, dass sie von einer **zweckwidrigen Weitergabe ihrer Unternehmensdaten über Mobilgeräte betroffen waren.**
- **Bei 16 %** geschah dieser Vorfall im Zusammenhang mit einer **Datenschutzverletzung.**

Warum ist die Sicherheit von mobilen Geräten so wichtig?

Die meisten Menschen sind mittlerweile von ihren mobilen Geräten sehr abhängig und zwar sowohl beruflich wie privat, wobei die Grenzen zwischen diesen beiden Bereichen zunehmend verschwimmen. Außerdem befinden sich auch mobile Bedrohungen weiter auf dem Vormarsch – vor allem Android-Geräte sind in Bezug auf den Bedrohungsschutz ganz erheblichen Herausforderungen ausgesetzt. Das gilt zunehmend auch für iOS.

Deshalb kommt der Sicherung mobiler Geräte eine ebenso große Bedeutung zu wie dem Schutz von Laptops und Workstations. Vielleicht sogar eine noch größere, weil Mitarbeiter immer häufiger remote arbeiten und ihre mobilen Geräte ebenso für soziale Interaktionen nutzen wie für die berufliche Kommunikation.

Mobile Device Security von Kaspersky

Aus diesen und anderen Gründen haben wir ein komplettes Modul zur Sicherung von mobilen Geräten, einschließlich der Privatgeräte von Mitarbeitern (BYOD), direkt in unsere Produkte und Lösungen für die Endpoint-Sicherheit aufgenommen: Kaspersky Endpoint Security Cloud für KMUs sowie Kaspersky Endpoint Security for Business für Großunternehmen.

Anforderungen der Unternehmen an die Sicherheit von mobilen Geräten

Für kleine und mittlere Organisationen ist im Rahmen der Kaspersky Endpoint Security Cloud der Schutz von 2 mobilen Geräte pro Nutzerlizenz bereits enthalten – so dass sowohl die geschäftlichen als auch die privaten mobilen Geräte der Mitarbeiter abgesichert sind. Unsere KMU-Kunden können ohne zusätzliche Kosten die Cybersicherheit ihre Mobilgeräte ebenso schützen wie die ihrer Mitarbeiter.

Die meisten Großunternehmen und Konzerne verfügen über eigene dedizierte Mobilitätsprogramme und stellen die notwendigen Budgets und Ressourcen dafür zur Verfügung. Deshalb erkennt und eliminiert unsere integrierte Endpoint-Lösung für Großunternehmen, einschließlich Kaspersky Endpoint Security for Business, nicht nur mobile Bedrohungen, sondern lässt sich außerdem komplett entsprechend den spezifischen Anforderungen konfigurieren und direkt in vorhandene Infrastrukturen und Tools wie Enterprise Mobility Management (EMM) integrieren.

Kompatibel mit den folgenden EMM-Lösungen:

- Microsoft Intune
- VMware AirWatch
- MobileIron
- IBM Maas360
- SOTI MobiControl
- sowie weitere AppConfig EMM-Plattformen

EMM-Integration

Enterprise Mobility Management-Lösungen (EMM) werden mittlerweile von vielen mittleren und großen Organisationen eingesetzt, weshalb sich die Funktionen zur Erkennung von mobilen Bedrohungen von Kaspersky auch problemlos neben den vorhandenen EMM-Plattformen nutzen lassen.

Funktionsliste von Kaspersky Mobile Device Security

Sicherheits- und Verwaltungsfunktionen für Android		
	Kaspersky Endpoint Security Cloud	**Kaspersky Endpoint Security for Business**
Bereitstellung/Upgrade	✓	✓
über Google Play	✓	✓
über separates Installationspaket	✗	✓
über EMM-Lösungen von Drittanbietern	✗	✓
Malware-Schutz mit Cloud-basierter Bedrohungsanalyse	✓	✓
Diebstahlschutz	✓	✓
Authentifizierung per PIN/Fingerabdruck	✓	✓
Remote-Befehle zum Orten, Sperren und Löschen	✓	✓
Compliance-Kontrolle	✓	✓
Rooting-Erkennung	✓	✓
Einhaltung der gesetzlichen Vorschriften für unterschiedliche Gerätetypen	✓	✓
Programmkontrolle	✓	✓
Kontrolle von Kamera, WLAN und Bluetooth	✓	✓
Webschutz/-kontrolle	✗	✓
Zustellung von Mail-/VPN-Zertifikaten	✗	✓
Android Enterprise/Exchange ActiveSync	✗	✓
Programmkonfiguration über EMM-Plattformen von Drittanbietern	✗	✓
Sicherheits- und Verwaltungsfunktionen für iOS		
Web-Schutz	✗	✓
Diebstahlsicherung (Sperren, Löschen)	✓	✓
iOS MDM-Profile	Nicht erforderlich	Vom Kunden verwaltet
iOS MDM-Server	✓	✓
Authentifizierung per PIN/Touch-ID/Gesichts-ID	✓	✓
Konfiguration von Proxy-Einstellungen	✓	✓
Webfilter	✓	✓
WLAN-Konfiguration	✓	✓
Programmrestriktionen und natives iOS-Funktionsmanagement	✓	✓
AirPlay-/AirPrint-Konfiguration	✓	✓
Konfiguration von E-Mail/Kalender/Kontakten	✓	✓
Einschränkungen für Medieninhalte	✗	✓
Zustellung von Mail-/VPN-Zertifikaten	✗	✓

Lizenzierung für Mobile Device Security

In Bezug auf die Lizenzierung möchten wir allen Unternehmen, ob groß oder klein, maximale Flexibilität bieten.

Jede Nutzerlizenz der Kaspersky Endpoint Security Cloud schließt den Schutz von 2 mobilen Geräten ein, so dass sowohl berufliche als auch private Geräte sicher verwendet werden können.

Jede Kaspersky Endpoint Security for Business-Lizenz kann auf ein beliebiges Gerät angewendet werden, egal ob Desktop, Server oder mobiles Gerät. Dieses sehr transparente Lizenzierungsmodell bedeutet, dass Kunden mit einer Vielzahl an zu sichernden Endpoints nicht die Anzahl eines jeden Gerätetyps zusammenzählen müssen. Es genügt die Gesamtzahl der Geräte, die geschützt werden sollen.

Neues über Cyberbedrohungen: https://de.securelist.com/
IT Security News: business.kaspersky.de
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise
Threat Intelligence Portal: opentip.kaspersky.de

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtert. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen Möglichkeiten nutzen können, die Technologien mit sich bringen. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Proven.
Transparent.
Independent.