KASPERSKY SECURITY FOR MOBILE

Lepší transparentnost pro správu a zabezpečení mobilních koncových zařízení — bez složitosti samostatného řešení.

Zavádění, správa a zabezpečení mobilního IT prostředí nemusí být ani komplikované ani nákladné. **S komponentou MDM (Mobile Device Management, tj. Správa mobilních zařízení)** je konfigurace zabezpečení mobilních zařízení bezproblémová a jednoduchá, přičemž na zařízení se instaluje **mobilní agent**, který zajišťuje nutnou ochranu před současnými hrozbami, a to i na zaměstnancem vlastněných zařízeních!

Hlavní rysy:

- PODPORA TABLETŮ A SMARTPHONŮ
- BEZDRÁTOVÉ POSKYTOVÁNÍ (OTA)
- ČASEM PROVĚŘENÉ ZABEZPEČENÍ MOBILNÍCH ZAŘÍZENÍ S NASAZENÍM AGENTA
- BEZPEČNÁ IMPLEMENTACE PRO APPLE MDM
- NATIVNÍ INTEGRACE S BEZPEČNOSTNÍM CENTREM KASPERSKY PRO KONFIGURACI, KONTROLU, REPORTING, INVENTARIZACI A NASTAVOVÁNÍ ZÁSAD

Podporované mobilní platformy:

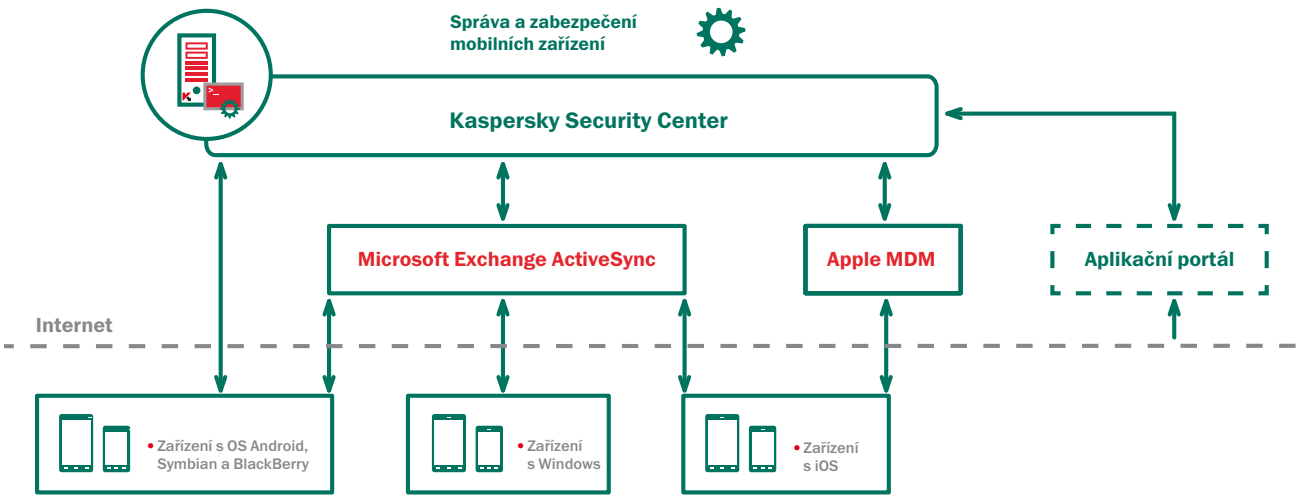
- iOS
- ANDROID™
- WINDOWS® PHONE
- WINDOWS MOBILE
- BLACKBERRY®
- SYMBIAN

VHODNÁ VOLBA PRO INICIATIVY BYOD („BRING YOUR OWN DEVICE“, TJ. PŘINESTE SI VLASTNÍ ZAŘÍZENÍ)

Řada zaměstnanců používá vlastní zařízení pro osobní i podnikové úkoly. Některé organizace dokonce podporují, aby si zaměstnanci vybrali jimi preferované smartphony nebo tablety v obchodě a IT oddělení zajistí přístup k e-mailům a podnikovým aplikacím z tohoto zařízení pracovníka.

Představuje to úspory a přínosy produktivity, ale tento přístup také může vystavit podnik bezpečnostním rizikům. Podniková data nevhodně zabezpečená a potenciálně promíchaná s osobními položkami lze snadno zneužít. Taková zařízení také bývají často používána členy rodiny, kteří nemají ponětí o zabezpečení aplikací. Některá zařízení jsou dokonce rootovaná nebo je na nich proveden jailbreak.

Kaspersky Security for Mobile řeší tyto problémy tím, že umožňuje bezpečnou konfiguraci a nasazování smartphonů a tabletů s použitím stejné konsole jako pro zabezpečení vaší sítě. Administrátoři IT si pak mohou být jisti, že uživatelská zařízení jsou konfigurovaná se správným nastavením a že je lze zabezpečit pro případ ztráty, krádeže nebo zneužití.



PODROBNÝ SEZNAM FUNKCÍ PRODUKTU KASPERSKY SECURITY FOR MOBILE:

FUNKCE PRO ZAJIŠTĚNÍ IT EFEKTIVITY:

JEDNODUCHÁ KONFIGURACE PROSTŘEDNICTVÍM JEDNÉ KONSOLE
Narozdíl od dalších řešení Kaspersky Lab administrátorům umožňuje používat pouze jednu konsoli pro správu zabezpečení mobilních zařízení, fyzických koncových zařízení, virtuálních systémů, šifrování a nástrojů pro uplatňování pravidel.

PRIVÁTNÍ PORTÁL APLIKACÍ
Administrátoři publikují obsah podnikového portálu, který obsahuje odkazy na schválené aplikace. Uživatelé mohou být omezeni pouze na použití těchto aplikací.

BEZDRÁTOVÉ POSKYTOVÁNÍ (OTA)
Vzdáleně zabezpečuje telefony buď odesláním e-mailu, nebo SMS s odkazem na podnikový portál, kam uživatelé mohou stahovat profil a vámi schválené aplikace. Přístup k datům nebude udělen, dokud je uživatel nepřijme.

BEZPEČNÁ KONFIGURACE
Zajišťuje softwarovou i hardwarovou integritu tím, že umožňuje detekci rootingu a jailbreaku. Mezi další bezpečnostní nastavení patří deaktivace kamery („camera disable“), vynucené heslo a další.

UPLATŇOVÁNÍ DODRŽOVÁNÍ PRAVIDEL A PŘEDEPSANÝCH NÁLEŽITOSTÍ
Kontrola aplikací umožňuje monitorování a kontrolu používání aplikací na zařízení včetně podpory „Default Deny“ (tj. implicitně odmítnout) a „Default Allow“ (tj. implicitně povolit).

KONTROLA BEZPEČNOSTNÍCH RIZIK:

ŠIFROVÁNÍ
Mobilní data jsou chráněna buď jako celý disk, nebo na úrovni souborů prostřednictvím transparentního šifrování, které lze také použít na zásobník.

PROTI KRÁDEŽI
Administrátoři mohou vzdáleně provádět plné nebo selektivní čištění zařízení, označit umístění chybějícího zařízení s hledáním pomocí GPS a získat informaci, zda došlo k odstranění nebo výměně SIM karty.

MOBILNÍ ANTIMALWARE
Antimalware engine společnosti Kaspersky Lab disponuje více úrovněmi detekce včetně ochrany s podporou cloudu a v kombinaci s bezpečným prohlížečem a výkonným antispamem zajišťuje, že nedojde k ohrožení zařízení škodlivým softwarem.

INTEGRITA PODNIKOVÝCH A OSOBNÍCH DAT:

ZÁSOBNÍKY
Pro podporu scénářů vlastních zařízení zaměstnanců lze podniková data a data aplikací umístit do samostatných zásobníků. Tím je zajištěna maximální bezpečnost pro podniková data a optimální integrita pro osobní obsah.

NÁSTROJE PRO BEZPEČNOST VZDÁLENÝCH DAT
V případě ztráty zařízení lze použít funkci Remote Lock (tj. vzdálený zámek). Podniková data v zásobníku na zařízení lze zabezpečit, šifrovat, provádět vzdáleně jejich správu a odstraňovat je nezávisle na osobních datech na daném zařízení.

Způsoby nákupu

Kaspersky Mobile Security je součástí těchto úrovní **Kaspersky Endpoint Security for Business**:

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

Kaspersky Security for Mobile si můžete zakoupit i samostatně. Pro bližší informace o produktu, kontaktujte vašeho prodejce.

NE VŠECHNY FUNKCE JSOU K DISPOZICI NA VŠECH PLATFORMÁCH.
Pro další informace navštivte **www.kaspersky.com**

KESB-MOBILE/Version 0.3/Nov12/Global

KASPERSKY lab