KASPERSKY SECURITY FOR MOBILE

Ökad hanteringssynlighet och -säkerhet för mobila klienter – utan den komplexitet som en separat lösning innebär.

Det behöver inte var komplicerat och dyrt att driftsätta, hantera och säkra företagets mobila IT-miljö. **Med Mobile Device Management (MDM)** är det enkelt att konfigurera säkerheten för mobila enheter, samtidigt som en **mobil agent** installeras på enheten för att ge det skydd som behövs mot dagens hot – även på anställdas privata enheter!

Huvudfunktioner:

- STÖD FÖR SURFPLATTOR OCH SMARTA TELEFONER
- DISTRIBUTION VIA FJÄRRANSLUTNING (OTA)
- BEPRÖVAD, AGENTBASERAD MOBILSÄKERHET
- SÄKER IMPLEMENTERING AV APPLE MDM OCH MICROSOFT EXCHANGE ACTIVESYNC
- INBYGGD INTEGRERING MED KASPERSKY SECURITY CENTER FÖR KONFIGURATION, KONTROLL, RAPPORTERING, INVENTERINGAR OCH UPPRÄTTANDE AV REGLER

Mobila plattformar som stöds:

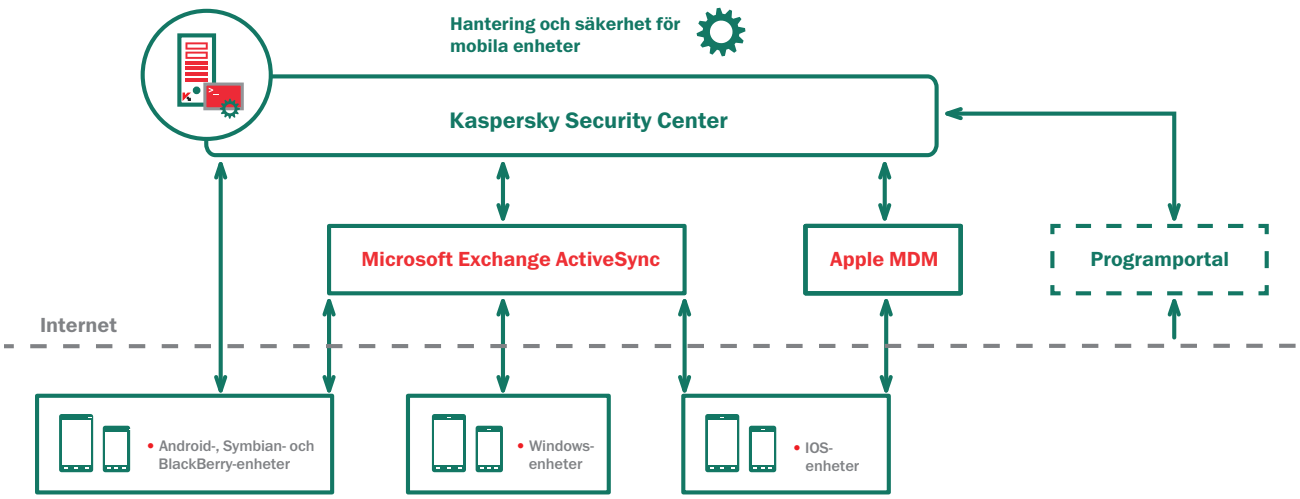
- IOS
- ANDROID™
- WINDOWS® PHONE
- WINDOWS MOBILE
- BLACKBERRY®
- SYMBIAN

PERFEKT FÖR LÖSNINGAR DÄR ANSTÄLLDA SKA KUNNA ANVÄNDA PRIVATA ENHETER (BYOD, BRING YOUR OWN DEVICE)

Många anställda använder sina privata enheter för både personliga och arbetsrelaterade ändamål. Vissa företag uppmuntrar till och med sina anställda att välja en smart telefon eller surfplatta hos en återförsäljare, och därefter förbereder IT-personalen den privatägda enheten för åtkomst till e-post och företagsnätverket.

BYOD kan ge besparingar och produktivitetsfördelar men kan även innebära att organisationen utsätts för säkerhetsrisker. Företagsdata som inte är korrekt skyddade och som potentiellt lagras tillsammans med privat material kan lätt utnyttjas. Dessa enheter används också ofta av familjemedlemmar som inte tänker på säkerheten vid programanvändning. Vissa enheters säkerhetssystem har rotats eller modifierats.

Kaspersky Security for Mobile löser dessa problem med hjälp av säker konfiguration och distribution för smarta telefoner och surfplattor via samma konsol som företagets nätverkssäkerhetssystem. IT-administratörer kan vara säkra på att användarnas enheter har konfigurerats med de korrekta inställningarna och är skyddade i händelse av förlust, stöld eller oförsiktig användning.



DETALJERAD INFORMATION OM FUNKTIONER I KASPERSKY SECURITY FOR MOBILE:

FUNKTIONER FÖR IT-EFFEKTIVITET:

ENKEL KONFIGURATION VIA EN ENDA KONSOL
Till skillnad från andra lösningar har Kaspersky Lab bara en konsol som administratörerna använder för att hantera säkerheten för mobila enheter, fysiska klienter, virtuella system, kryptering och verktyg för policyefterlevnad.

PRIVAT PROGRAMPORTAL
Administratörerna publicerar en företagsportal som innehåller länkar till godkända program. Användarna kan vara begränsade till enbart dessa program.

DISTRIBUTION VIA FJÄRRANSLUTNING
Telefoners fjärranslutning kan säkras genom att en länk till företagsportalen skickas via e-postmeddelande eller SMS, där användarna kan hämta den profil och de program du har godkänt. Åtkomst till data beviljas inte förrän användaren har accepterat.

SÄKER KONFIGURATION
Ensures hardware and software integrity by enabling rooting and jailbreak detection. Andra säkerhetsinställningar omfattar bland annat inaktivering av kamera och lösenordstvång.

PROGRAMANVÄNDNING OCH POLICYEFTERLEVNAD
Med programkontroll kan programanvändningen övervakas och styras på enheten, inklusive funktioner för Neka som standard och Tillåt som standard.

KONTROLL AV SÄKERHETSRISKER:

KRYPTERING
Dataöverföringar skyddas via transparent datakryptering på disk- eller filnivå som även kan tillämpas på en behållare.

STÖLDSKYDD
Administratörer kan via fjärranslutning utföra en fullständig rensning av en enhet eller delar av den, lokalisera en saknad enhet med GPS-sökfunktionen och även få meddelanden om ett SIM-kort tas ur eller byts ut.

SKYDD MOT SKADLIG PROGRAMVARA FÖR MOBILA ENHETER
Sökmotorn i Kaspersky Labs skydd mot skadlig programvara arbetar med identifiering på flera nivåer inklusive molnbaserat skydd. Detta i kombination med en säker webbläsare och ett kraftfullt skräppostskydd säkerställer att enheten inte utsätts för skadlig programvara.

INTEGRITET FÖR FÖRETAGSDATA OCH PRIVATA UPPGIFTER:

CONTAINRAR
I de fall anställda använder egna enheter kan företagsdata och program placeras i isolerade ”behållare”. Denna metod ger maximal säkerhet för företagets data och optimal integritet för personligt innehåll.

FJÄRRVERKTYG FÖR DATASÄKERHET
Om en enhet förloras kan den fjärrlåsas. Företagsdata i en behållare på enheten kan säkras och krypteras samt hanteras och rensas via fjärranslutning oberoende av personlig information som finns på enheten.

Hur du köper

Kaspersky Mobile Security ingår för de här användarna av **Kaspersky Endpoint Security for Business**:

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

Kaspersky Security for Mobile kan även köpas separat. Kontakta din återförsäljare för mer information och pris.

ALLA FUNKTIONER ÄR INTE TILLGÄNGLIGA PÅ ALLA PLATTFORMAR. Mer information finns på **www.kaspersky.se**

KASPERSKY LAB AB
JAN STENBECKS TORG 17
164 40 KISTA
SVERIGE
CORPORATESALES@KASPERSKY.SE
WWW.KASPERSKY.SE

KESB-MOBILE/Version 0.3/Nov12/Global

KASPERSKY lab