

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT



Fájlszervervédelemmel, végpontfelügyelettel és mobilvédelemmel (MDM)

A többretegű biztonság érdekében a mobil eszköz-felügyelet és a finomra hangolható végpontvédelmi eszközök egyesülnek a kártékony programok elleni védelemmel, az alkalmazottak által birtokolt mobil eszközökön is. A fájlserver védelme biztosítja, hogy a fertőzés a tárolt adatokon keresztül ne terjedhessen tovább a biztosított végpontokra.

VÉGPOINTFELÜGYELET

Alkalmazásfelügyelet – a Kaspersky Security Network által valós időben szolgáltatott fájlinformációk a dinamikus engedélylisták segítségével lehetővé teszik a rendszergazdák számára az alkalmazások engedélyezését, blokkolását vagy korlátozását, beleértve az „alapértelmezett letiltást”. Az alkalmazásjogosultság-vezérlés figyel és korlátozza az alkalmazások gyanús tevékenységeit.

Internetfelügyelet – böngésző szabályokat hozhat létre a nem megfelelő webhelyek előre beállított vagy személyre szabott adatbázisai alapján, és követheti a felhasználó tevékenységeit a vállalati hálózaton vagy roaming közben.

Eszközfelügyelet – lehetővé teszi a felhasználók számára, hogy beállítsák, ütemezzék és betartassák azokat az adatvédelmi eljárás módokat, amelyek az eltávolítható tárolóeszközök, illetve bármely más perifériák buszokra való csatlakoztatására vonatkoznak.

MOBILBIZTONSÁG:

Kártékony programok elleni védelem mobil eszközökhöz – kombinált proaktív, aláírás- és felhőalapú technológiák a hatékony, valós idejű mobil eszköz-védelem érdekében. Egy biztonságos böngésző és a levélzet elleni védelem növeli a biztonságot.

Mobil eszköz menedzsment (MDM) – A Kaspersky Security for Mobile támogatja a Microsoft Exchange ActiveSync, az Apple MDM és a Samsung SAFE funkcióit.

Lopás elleni távoli védelem – SIM-figyelés, távoli zárolás, teljes vagy szelektív törlés és keresés: mindegyik megakadályozza az illetéktelen hozzáférést a készülékhez lopás vagy elvesztés esetén.

Mobil eszközök felügyelete – a rendszergazdák nemcsak irányíthatják, hanem korlátozhatják is a különféle alkalmazások használatát, amivel megakadályozzák a nemkívánatos vagy „szürke” szoftverek alkalmazását. A rosszindulatú webhelyek letiltása mellett korlátozhatják a munkahelyi előírásoknak nem megfelelő weboldalakhoz való hozzáférést is.

Alkalmazások elkülönítése a BYOD program számára –

a vállalati adatok és alkalmazások elkülöníthetők az alkalmazottak személyes fájljaitól a vállalati alkalmazások speciális konténerbe helyezésével, amelyeket a személyes adatoktól függetlenül lehet titkosítani és – szükség esetén – távolról törölni.

FÁJLKISZOLGÁLÓK VÉDELME

A fájlservervédelem – amelynek vezérlése a végpontvédelemmel együtt a Kaspersky Security Centeren keresztül történik – biztosítja, hogy a kártékony programok ne tudjanak továbbterjedni a biztosított végpontokra a tárolt, fertőzött adatokon keresztül.

A Kaspersky Endpoint Security for Business – Select tartalmazza a Core változat minden komponensét.