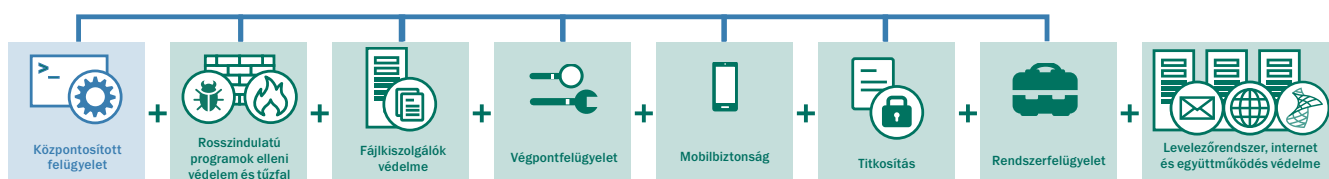
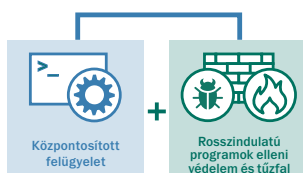


# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Az iparág vezető biztonsági szakértői által kifejlesztett és felépített erős, többszintű védelmi rendszer az ismert, ismeretlen és speciális fenyegetésekkel szemben. A világhírű fenyegetésfelderítést alkalmazó Kaspersky Endpoint Security for Business páratlan IT-biztonságot és felügyeletet biztosít.



# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS – CORE



## A kategóriában elérhető legjobb védelem a rosszindulatú programok ellen – a Kaspersky Lab biztonsági platform alapja

A Kaspersky Lab többszintű védelmi technológiáit saját, a biztonság mellett elkötelezett alkalmazottai fejlesztik. Az eredmény, amelyet a független tesztek is alátámasztanak: az iparág legerősebb és leghatékonyabb biztonsági megoldása – nincs ennél biztosabb védelem szervezete számára.

**Védelem az ismert, az ismeretlen és a speciális fenyegetések ellen** – az egyedülálló, kifinomult technológiák azonosítják és kiküszöbölik a meglévő és megjelenő fenyegetéseket.

**Támadások automatikus megelőzése** – proaktív módon célozza meg és azonosítja az ismeretlen és speciális fenyegetéseket.

**Felhőalapú védelem** – valós idejű információt használ a világhírű Kaspersky Security Network felhőalkalmazásokon keresztül.

**Rendszerfigyelő** – A rendszer támadása esetén egyedülálló fájl visszaállító funkciót kínál.

**Gazdagépalapú behatolásmegelőző rendszer (HIPS) személyes tűzfalal** – a HIPS az alkalmazás megbízhatósági szintje alapján korlátozza a rendszer tevékenységeit – egy, a hálózati aktivitást korlátozó, alkalmazásszintű személyes tűzfal segítségével.

# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT



## Erős, szoros végpontfelügyelet a mobileszközök és az adatok proaktív védelmével és kezelésével

Az alkalmazás-, internet- és eszközfelügyelet, a Kaspersky saját, egyedülálló laboratóriuma által támogatott dinamikus engedélyezést is beleértve, új dimenziót nyit a magas fokú végpontvédelem terén. A Kaspersky Security Center konzolon keresztül minden vállalati és az alkalmazottak tulajdonában álló (BYOD) mobileszköz védelme biztosítható, és minden platform egységesen kezelhető a védett végpontokkal együtt. A fájlkiszolgálók védelme biztosítja, hogy a fertőzés a tárolt adatokon keresztül ne terjedhessen tovább a biztosított végpontokra.

### VÉGPOINTFELÜGYELET

**Alkalmazásfelügyelet és dinamikus engedélyezés** – 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” egy élő vagy tesztkörnyezetben. Az alkalmazásjogosultság-vezérlés és a biztonságírás-keresés folyamatosan figyeli az alkalmazásokat, és korlátozza a gyanús tevékenységet folytató programokat.

**Internetfelügyelet** – az előre meghatározott vagy testre szabott kategóriák alapján létrehozható böngészési irányelvek átfogó felügyeletet és hatékony adminisztrációt eredményeznek.

**Eszközfelügyelet** – beállíthatja, beütemezheti vagy kényszerítheti a cserélhető tárolóeszközök és egyéb perifériás eszközök csatlakozását szabályozó adatszabályokat, maszkok használatával pedig egyszerre több eszközön is alkalmazhatja azokat.

### FÁJLKISZOLGÁLÓK VÉDELME

A Kaspersky Security Centeren keresztül a végpontvédelemmel együtt kezelve.

### MOBILBIZTONSÁG:

**Hatékony védelem a mobileszközökhöz** – fejlett, proaktív és felhőalapú technológiák kombinációja a többszintű, valós idejű mobilvégpont-védelemért.

**A webvédelmet, valamint a levélszemét és az adathalászat elleni védelmet szolgáló** komponensek tovább növelik az eszköz biztonságát.

**Lopás elleni távoli védelem – zárolás, törlés, helymeghatározás, SIM-figyelés, riasztás, fényképes azonosítás, teljes vagy szelektív törlés:** ezek mindegyike megakadályozza az illetéktelen hozzáférést a készülék tartalmához lopás vagy elvesztés esetén. A rendszergazda- és végfelhasználó-engedélyezés, valamint a Google Cloud kezelési támogatás szükség esetén gyors aktiválást tesz lehetővé.

### Mobilalkalmazás-felügyelet (MAM) –

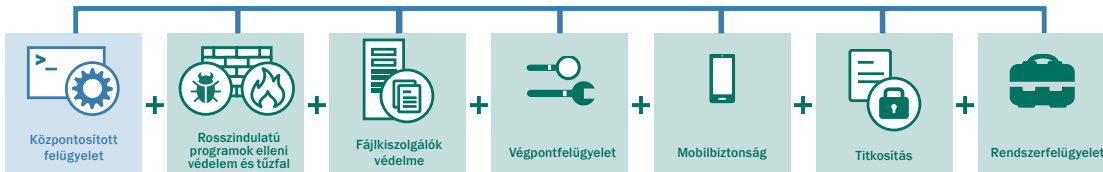
Az engedélyezett alkalmazások futtatására korlátozza a felhasználót, így megakadályozza a nem kívánatos vagy ismeretlen szoftverek telepítését. Az „Application Wrapping” elkülöníti a vállalati adatokat az alkalmazottak saját eszközein. További titkosítás vagy a „szelektív törlés” távolról is aktiválható.

**Mobileszköz-kezelés (Mobile Device Management - MDM)** – egységesített felhasználói felület **Microsoft® Exchange ActiveSync** és **iOS MDM** eszközökhöz OTA (Over The Air) szabályzat alkalmazásával. A **Samsung KNOX** az Android™-alapú eszközökön támogatott.

**Önkiszolgáló portál** – lehetővé teszi, hogy az alkalmazottak regisztrálják jóváhagyott eszközeiket a hálózaton a szükséges tanúsítványok és kulcsok automatikus telepítésével, illetve a felhasználók/tulajdonosok vészhelyzetben aktiválhassák a lopásvédelmi funkciókat, ezzel csökkentve az IT rendszergazdák terhelését.

**A Kaspersky Endpoint Security for Business – SELECT a CORE változat minden komponensét tartalmazza.**

# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED



## A rendszerfelügyeleti eszközök optimális IT-hatékonyságot és védelmet biztosítanak, míg az integrált titkosítás megóvja az érzékeny adatokat

Az automatikus javításkezelés és az OS-kép kezelés, valamint a távoli szoftverdisztribúció és a SIEM integráció mind hozzájárul az egyszerűbb adminisztrációhoz, míg a hardver- és a szoftvernyilvántartó leltárak és licenckelző eszközök átláthatóságot és megfelelő felügyeletet biztosítanak. Az integrált titkosítási technológia egy további, erős védelmi szintet biztosít.

### RENDSZERFELÜGYELET

**Biztonsági rések és biztonsági frissítések kezelése** – automatikus biztonságrés-érzékelés és -rangsorolás az operációs rendszerben és az alkalmazásokban, valamint a javítások és a frissítések gyors és automatikus szétosztása.

**Operációs rendszer telepítése** – operációs rendszer „golden” képeinek egyszerű létrehozása, tárolása, telepítése egy központi helyről.

**Szoftverdisztribúció és hibaelhárítás** – távoli szoftvertelepítés és alkalmazás, valamint igény szerinti vagy ütemezett operációsrendszer-frissítés, beértve a Wake-on-LAN támogatást is. Időtakarékos távoli hibaelhárítás és hatékony szoftverdisztribúció-támogatás a Multicast technológián keresztül.

**Hardver- és a szoftvernyilvántartó leltárak és licenckelzés** – az azonosítás, a láthatóság és a felügyelet (a blokkolást beleértve), valamint licenchasználat-kezelés a teljes környezetben használt valamennyi szoftver és hardver, többek között a cserélhető eszközök ellenőrzését is lehetővé teszi. Szoftver- és hardverlicenckelzés, vendégeszköz-érzékelés, jogosultságvezérlés és hozzáféréskiosztás is elérhető.

**SIEM integráció** – támogatás IBM® QRadar és HP ArcSight SIEM rendszerekhez.

**Szerepköralapú hozzáférés-vezérlés (RBAC)** – Adminisztratív felelősségi körök kiosztása teljes összetett hálózatokban, a kiosztott szerepeknek és jogoknak megfelelően testre szabott konzol nézetekkel.

### TITKOSÍTÁS

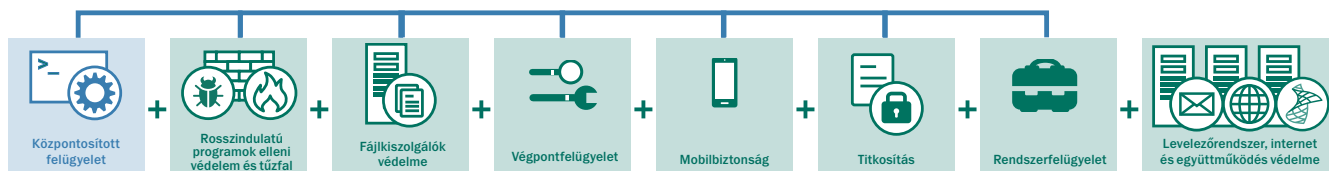
**Hatékony adatvédelem** – Fájl/mappa (FLE) és teljes lemezes (FDE) titkosítás is alkalmazható a végpontokon. A „hordozható mód” támogatása lehetővé teszi az adminisztratív tartományt elhagyó eszközök titkosításának adminisztrálását.

**Rugalmas felhasználói bejelentkezés** – A megnövelt biztonságot szolgáló, indítás előtti hitelesítés (PBA) opcionális „egyszeri belépési” lehetőséget tartalmaz a felhasználók átláthatósága érdekében. Kéttényezős vagy tokenalapú hitelesítés is rendelkezésre áll.

**Integrált irányelv létrehozása** – A titkosítás, valamint az alkalmazás- és eszközfelügyelet egyedülálló integrációja további biztonsági szintet nyújt és leegyszerűsíti az adminisztrációt.

**A Kaspersky Endpoint Security for Business – ADVANCED emellett a SELECT és a CORE változat minden komponensét tartalmazza.**

# ▶ KASPERSKY TOTAL SECURITY FOR BUSINESS



## Azok a szervezetek, melyeknek átfogó biztonsági megoldásra van szükségük a teljes IT-környezet védelmére, mind a Kaspersky Total Security for Business megoldást választják

A Kaspersky Total Security for Business az iparág napjaink leginkább teljes körű védelmi platformját és felügyeletét nyújtja. A Kaspersky Total Security for Business hálózata minden réteget megvédi, és hatékony konfigurációs eszközöket tartalmaz annak érdekében, hogy felhasználói készüléktől és helytől függetlenül is produktívak maradjanak, a kártékony programok fenyegetései nélkül.

### LEVELEZŐKISZOLGÁLÓK VÉDELME

E-mail alapú fenyegetések, adathalász támadások és a levélszemét hatékony megelőzése felhőalapú, valós idejű frissítések használatával a kimagasló elfogási arányok és a hamis riasztások számának csökkentése érdekében. Az IBM® Domino® kártékony programok elleni védelmével. A DLP funkció a Microsoft Exchange rendszerhez külön vásárolható meg.

### AZ INTERNETES ÁTJÁRÓK VÉDELME

Biztonságos internetet biztosít a vállalaton belül a kártékony és a potenciálisan veszélyes programok automatikus eltávolításával a HTTP(S)/FTP/SMTP és a POP3 forgalomban.

### EGYÜTTMŰKÖDÉS-VÉDELEM

Minden kártékony programtól megvédi a SharePoint® kiszolgálókat és parkokat. A Sharepoint kiszolgálóhoz külön megvásárolható DLP funkció tartalom- és fájl szűrő opciót tartalmaz, azonosítja a bizalmas adatokat, és védelmet biztosít az adatok kiszivárgása ellen.

### BIZTONSÁG EGY KICSIT MÁSKÉPP

A Kaspersky Lab az alapvető értékünknek számító és minden tevékenységünket meghatározó Biztonsági Intelligenciának köszönhetően a piacon elérhető legerősebb rosszindulatú programok elleni védelmet biztosítja.

- Minden szinten technológia-központú vállalat vagyunk – kezdve a vezérigazgatónkkal, Eugene Kasperskyvel.
- Az évek során az IT-biztonsági szakértőkből álló elit gárdánk, a globális kutatási és elemzési csapat (GREAT) szakemberei elsőként fedezték fel a világ legveszélyesebb rosszindulatú fenyegetéseinek és célzott támadásainak jelentős részét.
- A világ számos nagyra becsült biztonsági és bűnüldözési szervezete támaszkodik szakértelmünkre.
- Mivel a Kaspersky Lab saját maga fejleszti és tökéletesíti az alapvető technológiáit, termékeink ennél fogva sokkal stabilabbak és hatékonyabbak lehetnek.
- A Kaspersky évről évre minden más forgalmazónál több független teszten vesz részt – és minden más forgalmazónál nagyobb arányban végzünk az első helyen!
- A legszélesebb körben elismert ipari elemzők – köztük a Gartner, Inc, a Forrester Research és az International Data Corporation (IDC) – számos kulcsfontosságú IT-biztonsági kategóriában vezetőként értékelnek minket.
- Több mint 130 OEM – többek között a Microsoft, a Cisco Meraki, a Juniper Networks, az Alcatel Lucent és sok más vállalat – használja technológiáinkat a saját termékeiben és szolgáltatásaiban.

Ettől vagyunk igazán jók!

A Kaspersky Endpoint Security for Business, megoldással kapcsolatos bővebb információért vegye fel a kapcsolatot viszonteladójával.

## A Kaspersky Endpoint Security for Business – SELECT a CORE változat minden komponensét tartalmazza.

Kaspersky Endpoint Security for Business/2015. február/Globális

© 2015 Kaspersky Lab. Minden jog fenntartva. A bejegyzett védjegyek és szolgáltatási védjegyek azok tulajdonosainak tulajdonát képezik. A Microsoft, a Windows Server és a SharePoint a Microsoft Corporation Egyesült Államokban és/vagy egyéb országokban alkalmazott védjegyei vagy bejegyzett védjegyei.

**KASPERSKY** Lab