KASPERSKY VÁLLALATI TERMÉKEK 2013

Vegye észre.

KASPERSKY lab

A KASPERSKY LAB-RÓL

A Kaspersky Lab a világ legnagyobb független biztonsági szoftvert gyártó vállalata. A lehető legjobb biztonsági informatikai megoldás az Ön vállalata számára, a kártékony programok elleni hatékony védelemnek, a rugalmas felügyeleti eszközöknek, a titkosítási technológiának és a rendszerfelügyeleti eszközöknek köszönhetően. A Kaspersky biztonság a végpontoktól a szerverekig és internetes átjárókig terjed, az egyedülálló tervezési megközelítés pedig azt jelenti, hogy valamennyi fizikai, virtuális és mobil eszközét a hálózat méretétől függetlenül egyetlen központi kezelőkonzolról biztosíthatja és felügyelheti. A Kaspersky technológiát világszerte alkalmazzák piacvezető informatikai gyártók és kiadók termékeiben és szolgáltatásaiban.

További információ: www.kaspersky.com, vagy www.kaspersky.hu

Antivírusokkal, kémprogram védelmi és anti-spam rendszerekkel kapcsolatos legújabb tudnivalókról, trendekről a www.securelist.com oldalon tájékozódhat.

AZ EGYETLEN IGAZÁN INTEGRÁLT BIZTONSÁGI PLATFORM AZ IPARÁGBAN

EGYETLEN KONZOL

A Kaspersky termékeit úgy terveztük, hogy a rendszergazda a teljes biztonsági rendszert — virtuális gépeket, fizikai és mobil eszközöket egyaránt — „egyetlen ablakon” keresztül szemlélheti és felügyelheti.

EGYETLEN PLATFORM

A Kaspersky Lab kifejlesztette saját konzoljait, biztonsági moduljait és eszközeit, ahelyett hogy más vállalatoktól vásárolná őket. Az azonos kódbázisból dolgozó programozók olyan technológiákat fejlesztettek ki, amelyek kommunikálnak és együttműködnek egymással. Az eredmény stabilitás, integrált irányelvek, hasznos jelentéskészítés és intuitív eszközök.

EGYETLEN KÖLTSÉG

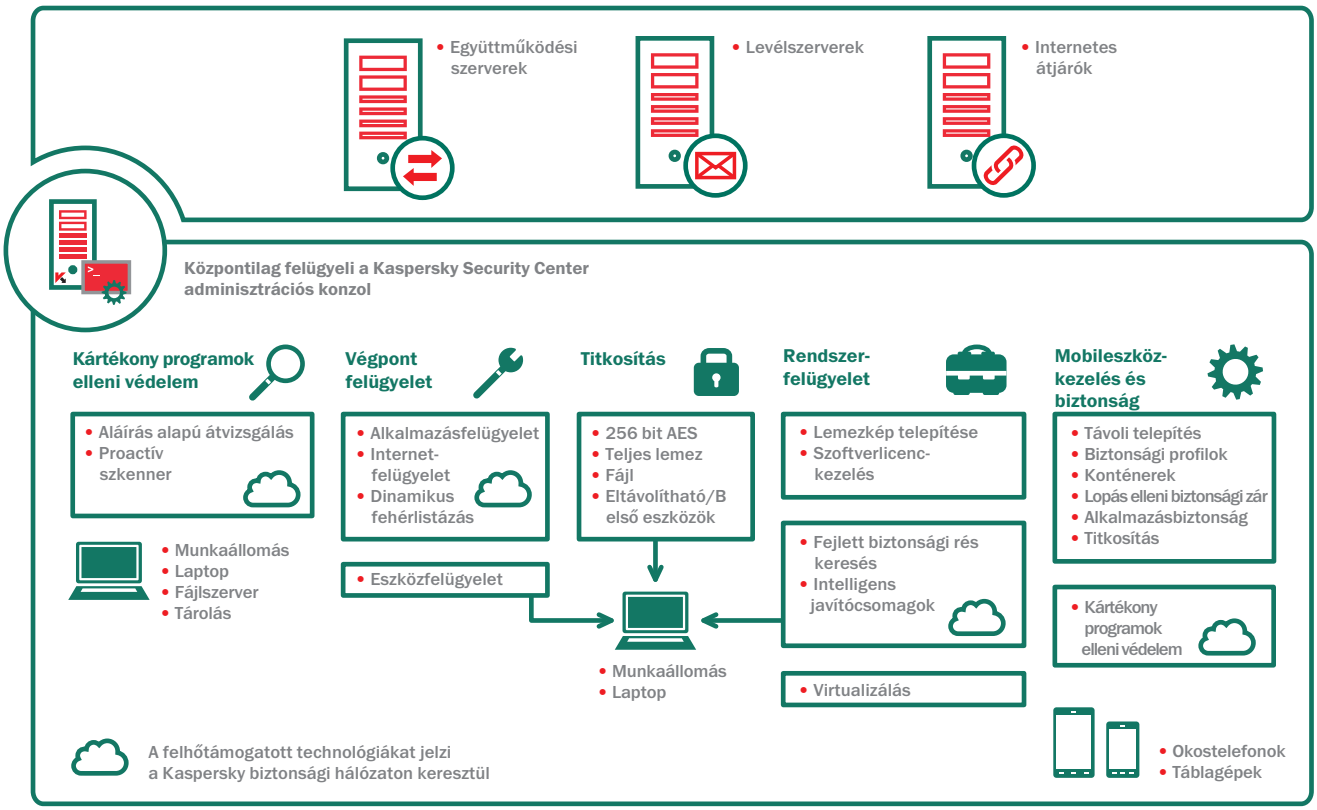
Egy adott telepítéshez tartozó összes Kaspersky termék és eszköz egyetlen értékesítőtől származik, — így nem kell minden alkalommal új költségvetési és igazolási folyamatot végrehajtani a biztonsági kockázatok és az Ön üzleti céljai összehangolása során.

A MEGFELELŐ MEGOLDÁS AZ ÖN SZÁMÁRA

A Kaspersky Security for Business a megfelelő megoldást kínálja az Ön vállalata számára – legyen szó akár a végpontok védelméről (munkaállomásoktól okostelefonokig és virtuális gépekig), a szerverek és internetes átjárók biztosításáról, illetve a teljes biztonsági környezet távfelügyeletéről.

A Kaspersky technológiák hosszú listájával büszkélkedhet, a titkosítástól és a mobil eszközök kezelésétől kezdve a hibajavító csomagkezelésig és licenc leltárokig. A felhőtámogatott Kaspersky biztonsági hálózat segítségével zökkenőmentesen működnek együtt, hogy ügyfeleink az általuk igényelt világszínvonalú védelmet élvezhessék az egyre kifinomultabb és szerteágazóbb „kiberfenyegetésekkel” szemben.

Röviden: alulról építkezve létrehoztuk az ágazat első biztonsági platformját, így a rendszergazdák könnyedén átláthatják, felügyelhetik és védhetik világukat.

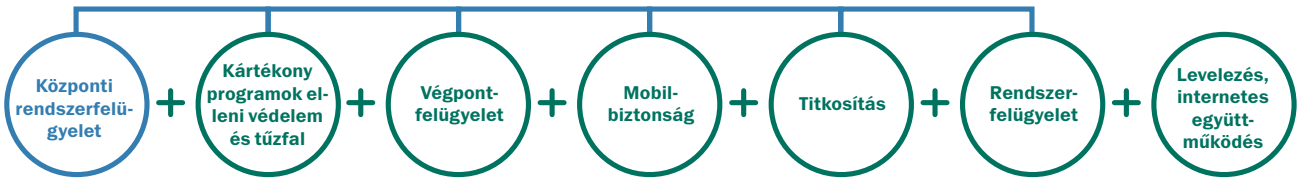


KASPERSKY SECURITY FOR BUSINESS

Technológiáink és együttműködésük

	Core	Select	Speciális	Total	A Security Center felügyeli	Célzott megoldásként rendelkezésre áll
Kártékony programok elleni védelem	•	•	•	•	•	
Tűzfal	•	•	•	•	•	
Alkalmazásfelügyelet		•	•	•	•	
Eszközfelügyelet		•	•	•	•	
Internetfelügyelet		•	•	•	•	
Fájlszerverek		•	•	•	•	•
Mobil végpontügynök		•	•	•	•	•
Mobileszköz-kezelés		•	•	•	•	•
Titkosítás			•	•	•	
OS képkezelés			•	•	•	•
Licenc felügyelet			•	•	•	•
Biztonsági rések felügyelete			•	•	•	•
Javítóprogramok kezelése			•	•	•	•
Hálózati hozzáférés szabályozása			•	•	•	•
Együttműködés				•		•
Levélszerverek				•		•
Internetes átjárók				•		•
Virtualizálás					•	•
Átjárás					•	•

KASPERSKY VÁLLALATI VÉGPONTBIZTONSÁG



CORE RÉTEG

Az alapokról indulva, ahol a Kaspersky díjnyertes, hatékony munkaállomása, kártékony programok elleni védelme és tűzfala található, megalkottuk intuitív ügyviteli konzolunkat, a Kaspersky Security Centert. Ezt a megoldást azoknak ajánljuk, akik csak a kártékony programok ellen kívánnak védekezni.

SELECT RÉTEG

A védelmi rendszerek listáján a CORE réteg jellemzői mellett **fájlszerver biztonság, alkalmazás fehérlistázás és felügyelet,** valamint **eszközvezérlés és a webes felügyelet** szerepel. Ide tartozik továbbá a **mobil védelmi megoldás,** amely egy **végpont-biztonsági ügynökből** és **mobileszköz-kezelésből (vagy MDM-ből) áll**. Amennyiben mobil munkaerejét kívánja védeni és informatikai irányelveit érvényesíteni, a SELECT az Ön számára a megfelelő réteg.

ADVANCED RÉTEG

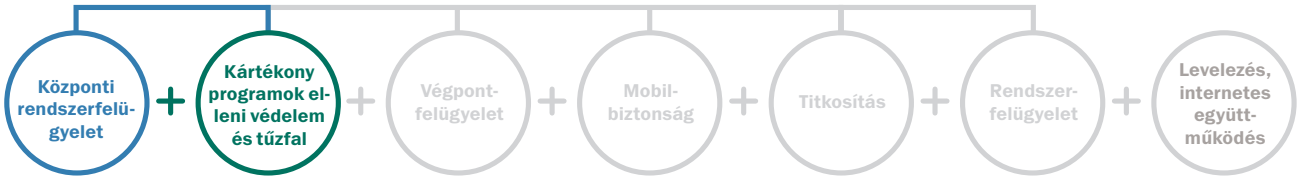
Az ADVANCED rétegben a Kaspersky fájl- vagy teljes lemezes **titkosítás** formájában kínál további **adatvédelmet**. Új ajánlatunk, a Kaspersky Systems Management a biztonságot és az informatikai hatékonyságot ötvözi. Ez a rengeteg funkció olyan lényeges eszközöket működtet, amelyekkel a rendszergazda:

- Az Image Management modul segítségével lemezképeket hozhat létre és rendszereket telepíthet.
- Fontossági sorrendbe rakhatja a hardver- és szoftver-sérülékenység vizsgálatát, hatékonyan ötvözve a fejlett sérülékenység-vizsgálattal és az intelligens javításkezeléssel.
- Nyomon követheti a licenchasználatot és a szoftverlicenc-kezelés betartását.
- A hálózati hozzáférés szabályozásával adat- és infrastruktúra-hozzáférési szabályzatokat állíthat be felhasználóknak és vendégeknek.
- A központi konzolról elvégezheti a frissítések és az új szoftverek távoli telepítését és installálását a felhasználók részére.

KASPERSKY TOTAL SECURITY FOR BUSINESS

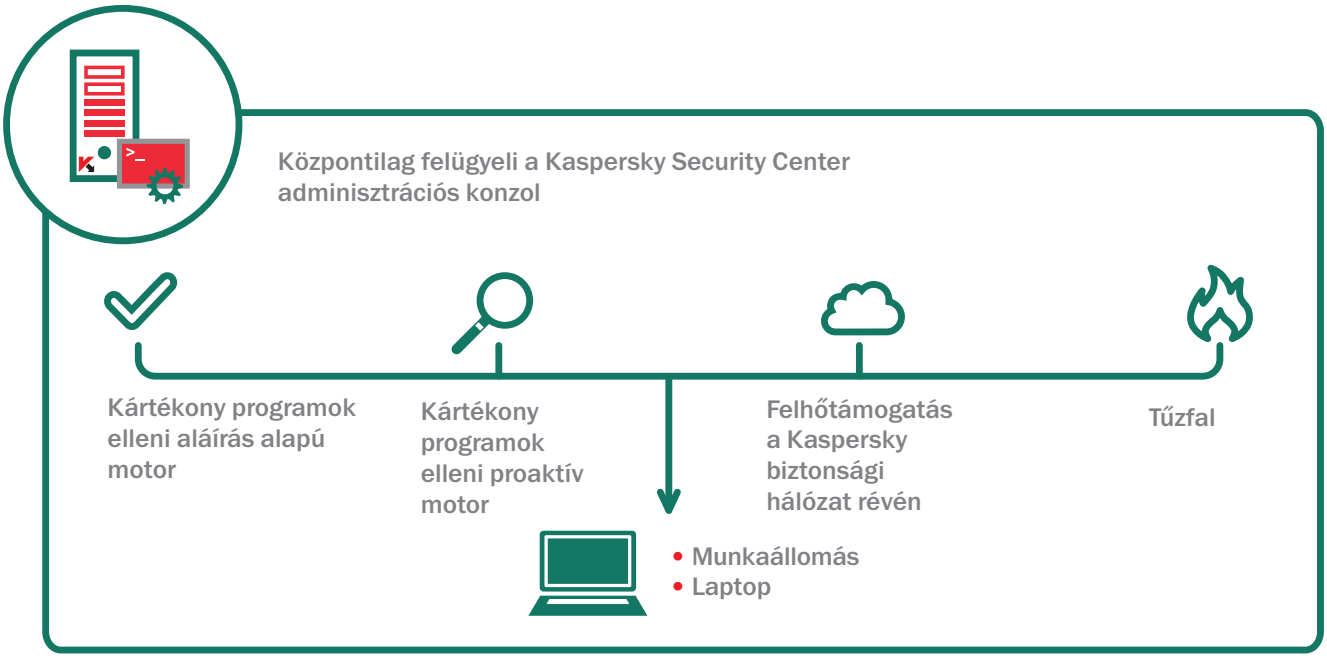
Legnépszerűbb termékünk, a Kaspersky Total Security for Business az összes előző réteg ötvözésével, a webes, a levelező és az együttműködési szerver további védelmével erősíti meg az Ön biztonsági helyzetét. Ez a megoldás azon komoly biztonsági igényeket megfogalmazó cégek számára tökéletes, amelyek mindegyik hálózati szinten a legjobb védelemre vágynak.

KASPERSKY VÁLLALATI VÉGPONTBIZTONSÁG
Core



Díjnyertes kártékony programok elleni védelem központi telepítéssel, felügyelettel és jelentéskészítéssel.

A többszintű biztonsági modell alapja a legjobb kártékony programok elleni védelem. Mivel a Kaspersky hosszú ideje piacvezető a kártékony szoftverek felismerésében és eltávolításában, nincs ennél jobb alap. A Kaspersky Endpoint Security for Business „Core” szintet a Kaspersky Security Center központilag kezeli, és a felhőtámogatott Kaspersky biztonsági hálózat támogatja.



Kaspersky Endpoint Security for Business, Core réteg — Kártékony programok elleni erős védelem, felhőtámogatott védelemmel.

KULCSFONTOSSÁGÚ JELLEMZŐK:

KÁRTÉKONY PROGRAMOK ELLENI HATÉKONY VÉGPONTFELÜGYELET
A Kaspersky ellenőrző motorjai több szinten működnek az operációs rendszerben, a kártékony programok felismerésében.

FELHŐ KOMPATIBILIS VÉDELEM
A felhő alapú Kaspersky biztonsági hálózatban a felhasználók valós időben élveznek védelmet az új fenyegetésekkel szemben.

KÖZPONTI RENDSZERFELÜGYELET
A rendszergazdák központilag eltávolítják a meglévő vírusirtó szoftvereket, konfigurálhatják és telepíthetik a Kaspersky szoftvert és elvégezhetik a jelentéskészítést — mindezt ugyanarról a konzolról.

KÁRTÉKONY PROGRAMOK ELLENI VÉGPONTI FUNKCIÓK:

GYAKORI FRISSÍTÉSEK ÉS ALÁÍRÁS ALAPÚ VÉDELEM
Az iparágban bevált, hagyományos aláírás alapú módszer a kártékony programok veszélyeinek észlelésére.

VISELKEDÉSELEMZÉS VÉGREHAJTÁSA A RENDSZERFELÜGYELŐVEL
A Kaspersky biztonsági hálózat (KSN) a hagyományos védelmi módszereknél sokkal gyorsabban reagál a veszélygyanús helyzetekre. A KSN reakcióideje egy kártékony programmal szemben akár 0,02 másodperc!

HOSZT ALAPÚ BEHATOLÁS-MEGELŐZŐ RENDSZER (HIPS) ÉS SZEMÉLYES TŰZFAL
A leggyakoribb alkalmazások százaira vonatkozó, előre meghatározott szabályok jóvoltából hamarabb konfigurálható a tűzfal.

SZÉLES KÖRŰ MULTIPLATFORM TÁMOGATÁS
A Kaspersky szoftver végponti biztonságot kínál Windows®-hoz, Macintosh® -hoz és Linux®-hoz, megkönnyítve a különböző hálózatokat felügyelő rendszergazda munkáját.

A KASPERSKY SECURITY CENTER JELLEMZŐI:

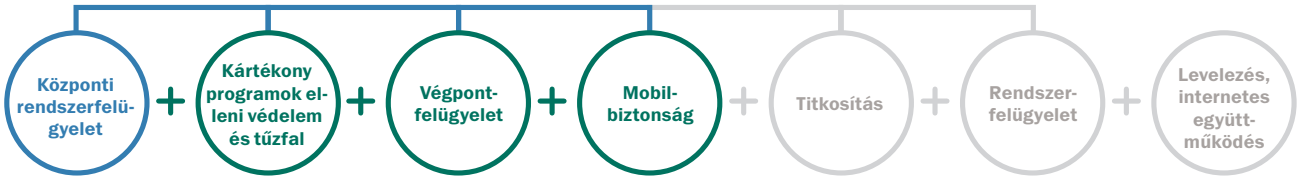
EGY KÖZPONTI KONZOL
Távoli felügyelet a Kaspersky által védett valamennyi végponthoz.

INTUITÍV FELHASZNÁLÓI INTERFÉSZ
A rendezett táblán megjelenő érthető, kezelhető információ segítségével az adminisztrátorok ellenőrizhetik a valós idejű védelmi státuszt, irányelveket állíthatnak fel, rendszereket kezelhetnek és jelentéseket fogadhatnak.

INTERNETES INTERFÉSZ
Távolról felügyeli a védelmi státuszt és hozzáférhető interfészről jelzi a kulcsfontosságú eseményeket.

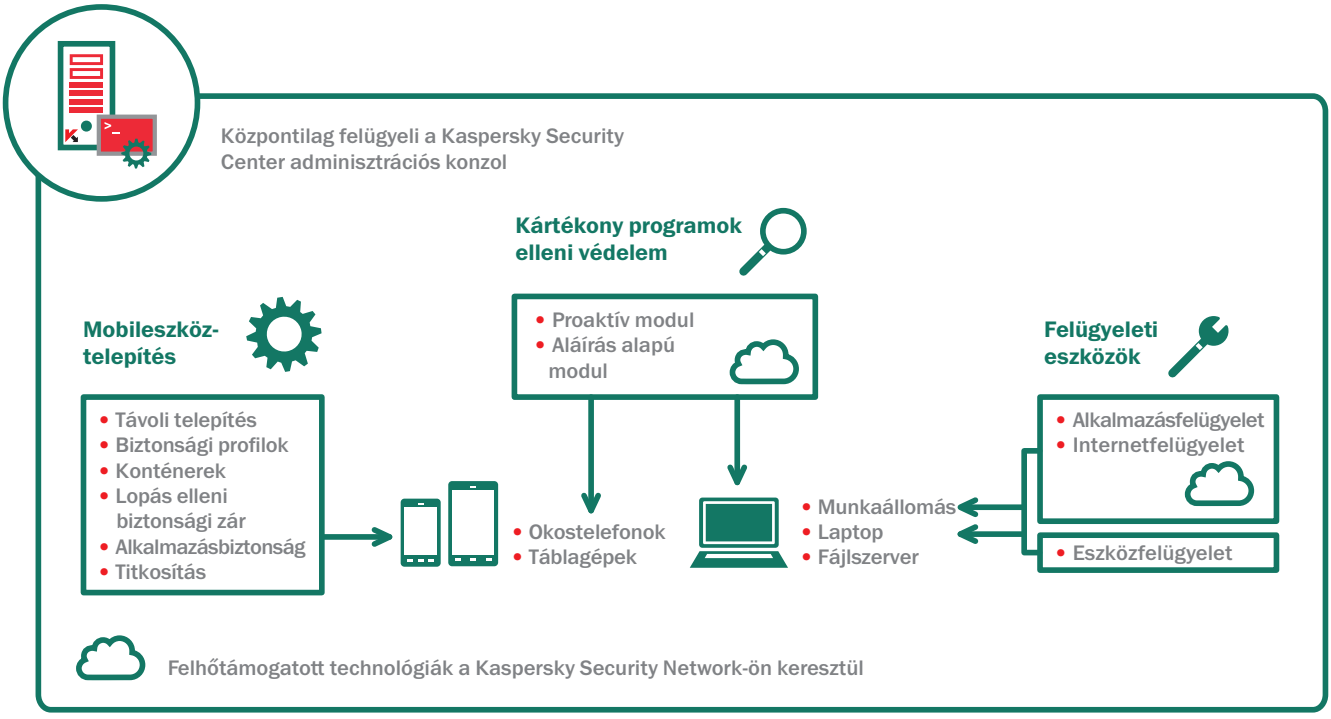
SKÁLÁZHATÓ TÁMOGATÁS
Az infrastruktúra méretétől függetlenül a Kaspersky Security Center konfigurációs, telepítő és kezelő eszközöket, rugalmas szabályzati opciókat és részletes jelentéseket kínál a felhasználó igényei szerint.

KASPERSKY VÁLLALATI VÉGPONTBIZTONSÁG
Select



A mobil munkaerő biztosítását szolgáló eszközök biztosítják az informatikai biztonsági megfelelőséget és blokkolják a kártékony programokat.

A Kaspersky „Select” rétege a mobileszköz telepítést és a Mobileszközök felügyeletén (MDM) és a kártékony programok elleni védelmen keresztül mobil védelmet foglal magában. Végpont felügyeleti eszközök (internet, eszköz és alkalmazás) segítenek a vállalatnak az informatikai irányelvek érvényesítésében, ezáltal megőrizve az Ön informatikai környezete legfontosabb elemeinek biztonságát.



Kaspersky Endpoint Security for Business — Select réteg Felügyeleti eszközök és mobilbiztonság.

KULCSFONTOSSÁGÚ JELLEMZŐK:

KÁRTÉKONY PROGRAMOK ELLENI HATÉKONY VÉGPONTFELÜGYELET
A Kaspersky szoftver legjobb ellenőrző motorjai több szinten működnek az operációs rendszerben, a kártékony programok felismerésében. A felhőalapú Kaspersky biztonsági hálózatban (KSN) a felhasználók valós időben élveznek védelmet az új fenyegetésekkel szemben.

RUGALMAS, ÁTFOGÓ FELÜGYELETI ESZKÖZÖK
A felhőalapú, biztonságos és nem biztonságos alkalmazások és internetes oldalak adatbázisa segít a rendszergazdának az alkalmazásokra és internetes szörfözésre vonatkozó irányelvek felállításában és érvényesítésében, míg az átfogó felügyeleti eszközök biztosítják, hogy kizárólag meghatározott eszközöket lehessen a hálózat gépeihez csatlakoztatni.

HATÉKONY MOBIL TELEPÍTÉS ÉS BIZTONSÁG OKOSTELEFONOKHOZ ÉS TÁBLAGÉPEKHEZ
Ügynökalapú mobil biztonság érhető el Android™, BlackBerry®, Symbian és Windows® mobileszközökhöz. A mobileszközökre vonatkozó irányelveket és szoftvereket távolról lehet telepíteni ezekre és az iOS eszközökre, a Kaspersky MDM-en keresztül.

EBBEN A RÉTEGBEN:

VÉGPONT FELÜGYELET:

ALKALMAZÁS FELÜGYELET
A rendszergazdák számára olyan irányelvek felállítását teszi lehetővé, amelyek engedélyezik, blokkolják vagy szabályozzák az alkalmazásokat (vagy alkalmazás kategóriákat).

ESZKÖZFELÜGYELET
A felhasználók számára lehetővé teszi az adatokkal kapcsolatos irányelvek felállítását, ütemezését és érvényesítését az eltávolítható tárolóeszközök és egyéb perifériaeszközök segítségével - USB-hez vagy egyéb busztípusokhoz csatlakoztatva.

INTERNETFELÜGYELET
Ez azt jelenti, hogy a végpont alapú szörfözési felügyelet követi a felhasználót - legyen szó akár a vállalati hálózatról, akár barangolásról.

DINAMIKUS FEHÉRLISTÁZÁS
A Kaspersky biztonsági hálózat által szolgáltatott valós idejű fájl reputációk biztosítják, hogy az Ön jóváhagyott alkalmazásai kártékony programoktól mentesek, és növelik a felhasználó hatékonyságát.

KASPERSKY SECURITY FOR MOBILE:

KÁRTÉKONY PROGRAMOK ELLENI INNOVATÍV TECHNOLÓGIÁK
Az aláírás alapú, proaktív és felhőtámogatott kimutatás ötvözete valós idejű védelmet eredményez. A biztonságos böngésző és a spam védelem növelik a biztonságot.

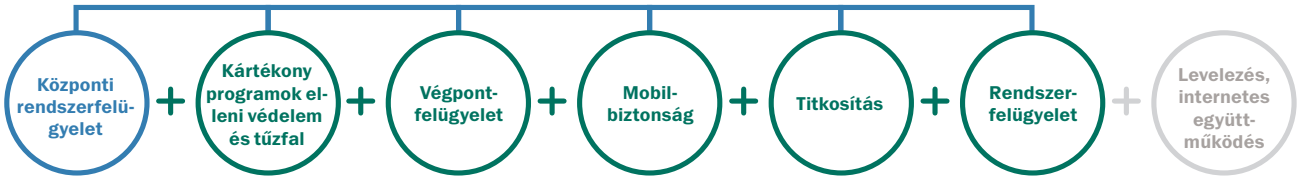
OTA (OVER THE AIR) TELEPÍTÉS
Előkonfigurálás és alkalmazások telepítése központilag, SMS, e-mail és számítógép segítségével.

LOPÁS ELLENI TÁVOLI ESZKÖZÖK
A SIM-Watch, a távoli zárolás és a Wipe and Find funkciók mind megakadályozzák a vállalati adatokhoz való illetéktelen hozzáférést a készülék elvesztése vagy ellopása esetén.

ALKALMAZÁSFELÜGYELET MOBILESZKÖZÖKHÖZ
Az előre meghatározott csoportirányelvek szerint felügyeli a mobileszközre telepített alkalmazásokat. Magában foglal egy „kötelező alkalmazás” csoportot.

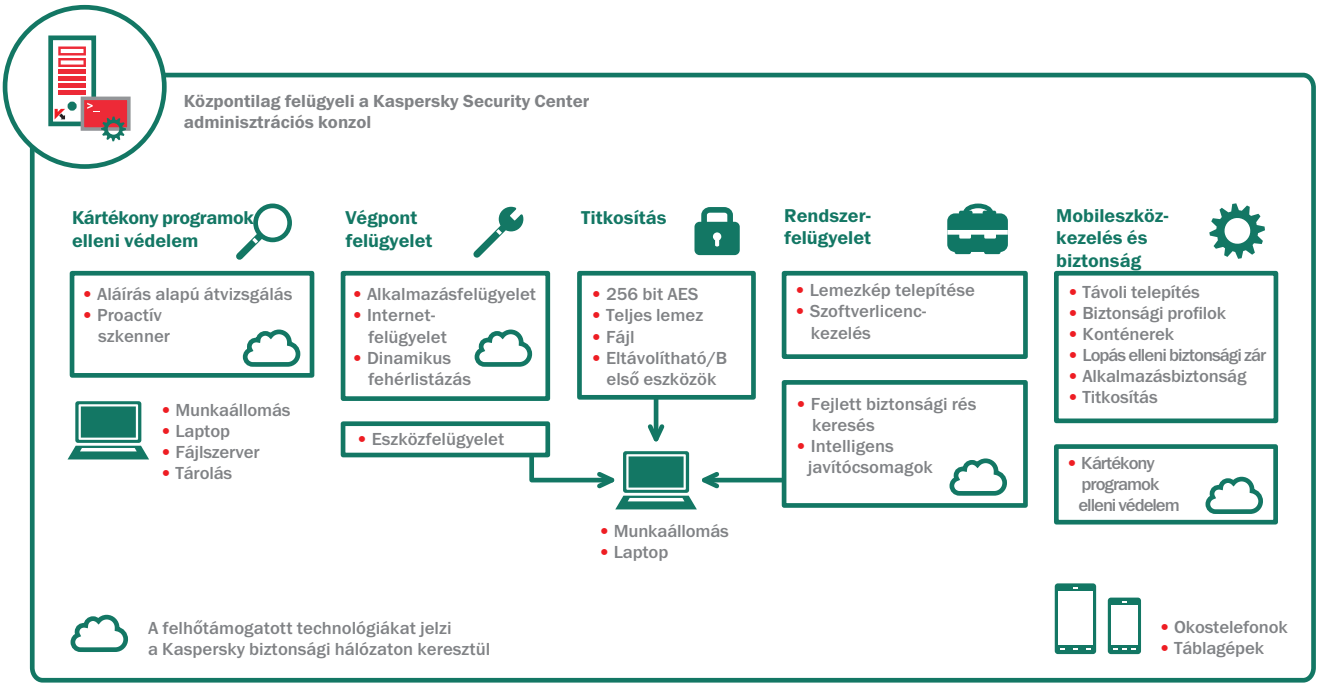
TÁMOGATÁS AZ ALKALMAZOTTAK SAJÁT ESZKÖZEIHEZ
A vállalati adatok és az alkalmazások titkosított konténerekben vannak elszigetelve, amelyek a felhasználó számára láthatóak. Ezek az adatok külön törölhetőek.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Speciális



A Kaspersky Lab megoldásainak sora bővelkedik biztonsági eszközökkel ötvözött informatikai optimalizálási jellemzőkben.

A Kaspersky Advanced rétege védelmet nyújt és felügyeleti megoldást kínál a vállalat igényeihez, az informatikai irányelvek érvényesítéséhez, a kártékony programok távol tartásához, az adatveszteség megelőzéséhez és az informatikai hatékonyság növeléséhez.



Kaspersky Endpoint Security for Business — Advanced szint. Titkosítási technológiával és biztonsági rendszer felügyelettel.

KULCSFONTOSSÁGÚ JELLEMZŐK:

HATÉKONY TITKOSÍTÁSI TECHNOLÓGIA
A teljes lemez- és mappaszintű AES 256-bites titkosítás véd az adatvesztés vagy adatlopás ellen, és lehetővé teszi a biztonságos adatmegosztást eltávolítható eszközökön, e-mailen, internetes hálózaton keresztül, mindezt a felhasználó számára láthatóan.

RENDSZER-KONFIGURÁCIÓ ÉS JAVÍTÓCSOMAG KEZELÉS
Az operációs rendszerek képének létrehozása és telepítése, biztonsági rések keresése, automatizált javítócsomag kezelése, hálózati hozzáférés vezérlése, leltárok és licenc kezelése egyetlen, egyszerű, felhasználóbarát központi kezelőfelületen át irányítható teljesen egységes rendszert alkotnak.

MOBIL TELEPÍTÉS ÉS BIZTONSÁG OKOSTELEFONOKHOZ ÉS TÁBLAGÉPEKHEZ
Ügynök alapú mobil végponti biztonság, valamint eszköz- és szoftverirányelvek távfelügyelete a Kaspersky MDM-en keresztül.

KÁRTÉKONY PROGRAMOK ELLENI HATÉKONY VÉGPONTFELÜGYELET ÉS RUGALMAS FELÜGYELETI ESZKÖZÖK
Kaspersky felhőtámogatott kártékony programok elleni legjobb védelem és átfogó alkalmazások, internet és eszköz felügyeleti eszközök.

EZEN A SZINTEN:

TITKOSÍTÁS ÉS ADATVÉDELEM:

ÁTFOGÓ TITKOSÍTÁS
Válasszon teljeslemezes vagy fájlszintű védelmet, a 256 bites titkosítású Fejlett Titkosítási szabvány (AES) támogatásával, a kritikus vállalati információk biztosításához, lopás vagy adatvesztés esetére.

BIZTONSÁGOS ADATMEGOSZTÁS
Hozzon létre titkosított és önkibontó csomagokat az adatvédelem biztosítása érdekében, eltávolítható eszközökön, e-mailen, hálózatban vagy interneten való megosztás esetén.

TÁMOGATÁS AZ ELTÁVOLÍTHATÓ ESZKÖZÖK SZÁMÁRA
Növeli a biztonságot olyan irányelvek segítségével, amelyek érvényesítik az eltávolítható eszközökön való adattitkosítást.

ÁTLÁTHATÓSSÁG A VÉGFELHASZNÁLÓK SZÁMÁRA
A Kaspersky titkosítási megoldása gördülékenyen működik, a felhasználók számára nem látható, a termelékenységet nem befolyásolja negatívan. Az alkalmazások beállításain vagy frissítésein sem változtat.

RENDSZERKONFIGURÁCIÓ ÉS JAVÍTÓCSOMAG-KEZELÉS:

JAVÍTÓPROGRAMOK KEZELÉSE
A biztonsági rések magas szintű, részletes átvizsgálása, a javítócsomagok automatikus elosztásával ötvözve.

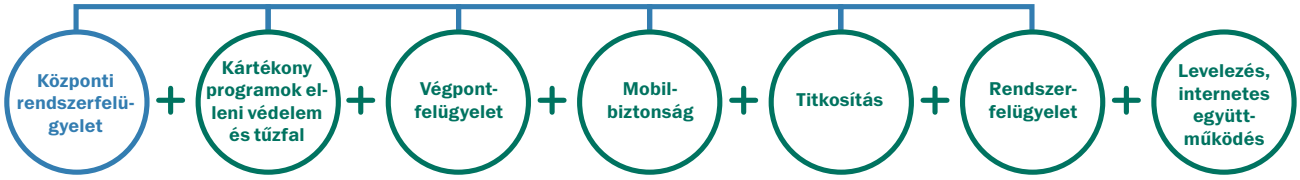
OPERÁCIÓS RENDSZEREKET ÉS ALKALMAZÁSOKAT TARTALMAZÓ LEMEZKÉPEK KEZELÉSE
Rendszerképek egyszerű létrehozása, tárolása és telepítése egy központi helyről. Tökéletes a Microsoft® Windows® 8-ra való áttéréshez.

TÁVOLI SZOFTVER TELEPÍTÉS
A szoftver központi telepítése az ügyfelek gépeire, akár fiókirodákban.

HÁLÓZATI BELÉPTETÉS-ELLENŐRZÉS (NAC)
A hálózati beléptetés-ellenőrzés (NAC) lehetővé teszi, hogy a hálózatra „látogatói” szabályokat állítsunk be. A vendégkészülékek (például mobilkészülékek) felismerése automatikusan megtörténik, és a rendszer átirányítja őket egy olyan céges portálra, ahol a megfelelő jogosultságok birtokában az általunk kijelölt erőforrásokhoz férhetnek hozzá.

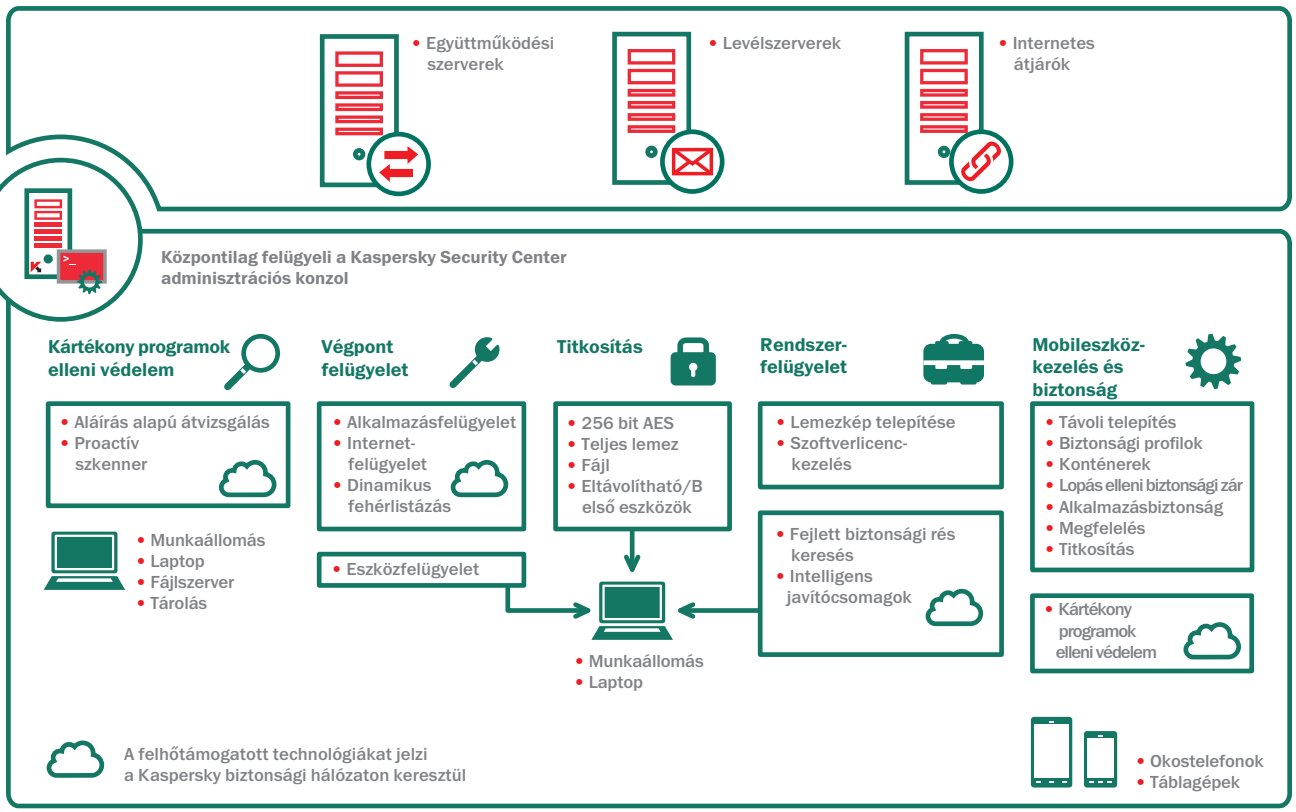
HARDVER, SZOFTVER ÉS LICENC FELÜGYELET
A hardver és szoftver leltárjelentések segítenek a licenckötelezettségek ellenőrzésében. Így a szoftverjogok központi kiosztásával költséget takaríthatunk meg.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Teljes körű védelem a kártékony programok ellen, titkosítás, átfogó informatikai hatékonyság és irányelv érvényesítési eszközök.

A Kaspersky Total Security for Business az iparágban ma elérhető legátfogóbb védelmi és felügyeleti platformot kínálja. A Total Security for Business a hálózat valamennyi szintjét biztosítja, és hatékony konfigurációs eszközöket tartalmaz a felhasználók hatékonyságának és a kártékony programoktól való védelmének érdekében, eszköztől és helyszíntől függetlenül.



KULCSFONTOSSÁGÚ JELLEMZŐK:

Az előző három réteg jellemzői, továbbá:

LEVÉLSZERVER VÉDELEM
Kártékony programok elleni védelem és a levélforgalom spamvédelme valamennyi levelezőrendszerhez

INTERNET ÁTJÁRÓK VÉDELME
Biztonságos internet-hozzáférés az egész szervezeten belül a HTTP(S)/FTP/SMTP és POP3 forgalom kártékony és esetlegesen veszélyes programjai automatikus eltávolításának köszönhetően.

BIZTONSÁGOS EGYÜTTMŰKÖDÉS
A Kaspersky megvédi a SharePoint® szervereket a kártékony programoktól, míg a tartalom- és fájlszűrési képességek segítenek a nem megfelelő tartalom tárolásának megelőzésében.

EZEN A SZINTEN:

LEVÉLSZERVEREK:

LEVÉLFORGALOM VÉDELME
Levelek védelme a levelezési és együttműködési platformok legújabb verzióiban: Microsoft Exchange, IBM Lotus Domino és Linux alapú levélszerverek.

KSN INTEGRÁCIÓ A SPAM VÉDELEM ÉRDEKÉBEN
A spam kimutatási aránya növekszik a Kaspersky Lab felhő alapú fenyegetésazonosítási motorjával (KSN) való integrációnak köszönhetően. identification engine (KSN).

FORGALOM JELENTETTE CSÖKKENTETT TERHELÉS
A felhőkompatibilis, intelligens spamszűrés jelentősen csökkenti a forgalom jelentette terhelést.

A RENDSZER ERŐFORRÁSAINAK OPTIMALIZÁLÁSA
Új antivírus motor, a szerver erőforrásai terhelésének kiegyenlítése és a vizsgálati kivételek alkalmazása együttesen csökkentik a rendszer terhelését.

INTERNETES ÁTJÁRÓK:

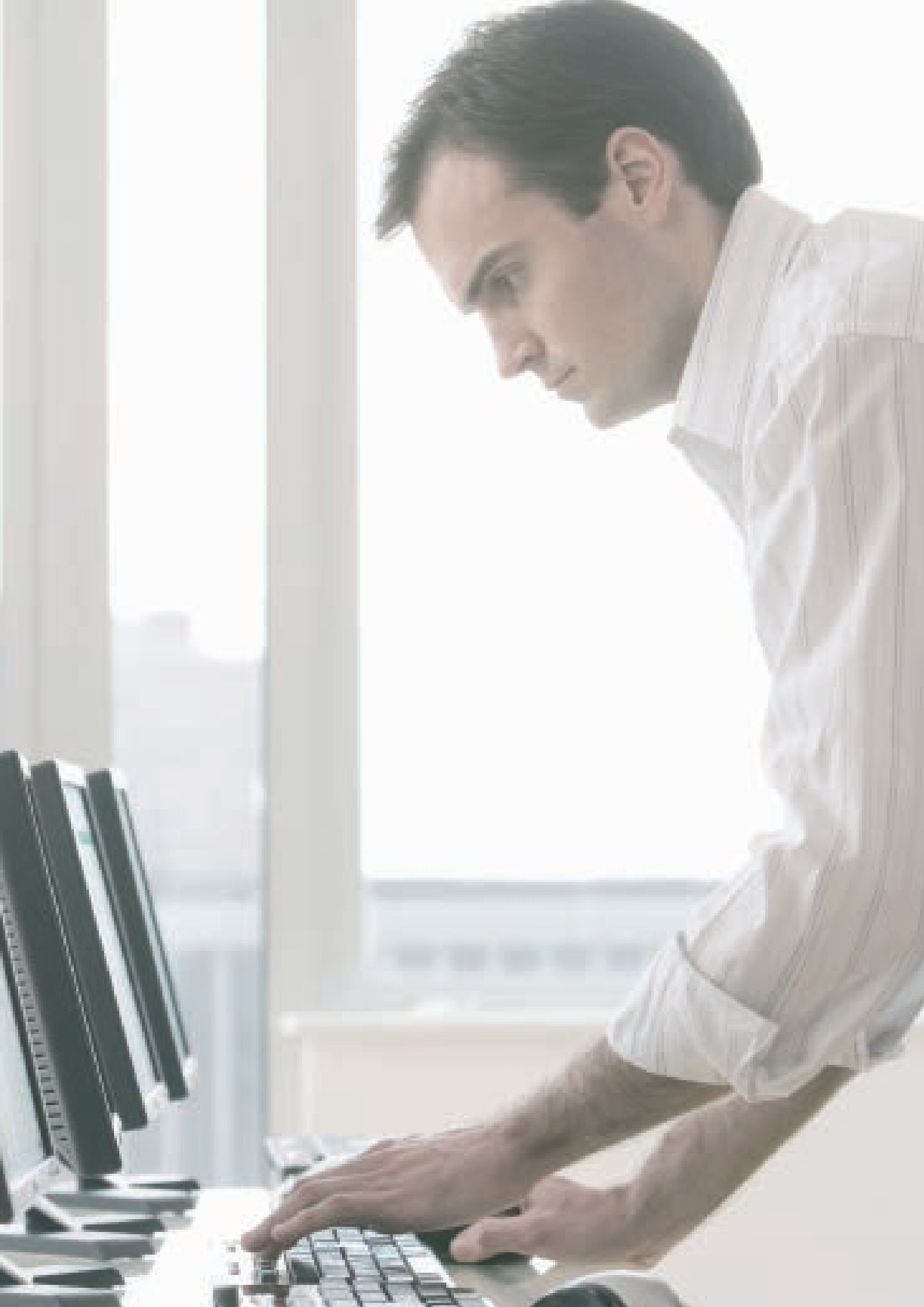
NAGY TELJESÍTMÉNY
A hatékony antivírus motor, továbbá az optimalizált, intelligens átvizsgálási technológia és a terheléskiegyenlítés növelik a teljesítményt, és csökkentik a vírusátvizsgáláshoz szükséges erőforrásokat.

MULTIPLATFORM TÁMOGATÁS
A Kaspersky Security for Internet Gateway támogatja a Windows és Linux platformokon működő legnépszerűbb internetes átjárókat.

EGYÜTTMŰKÖDÉS

KÁRTÉKONY PROGRAMOK ELLENI KORLÁT A SHARE POINT FARMOKHOZ
Az innovatív felismerési technológia azonosítja és blokkolja a kártékony programokat a valós idejű feltöltéseknél és letöltéseknél.

TARTALOMSZŰRÉS
Segít megakadályozni a nem megfelelő külső feltöltéseket, a belső kommunikációs irányelvek érvényesítésével, és blokkolja a nem megfelelő fájlok tárolását a fájltípus vagy szövegtartalom szerint.



KASPERSKY ANTI-VIRUS FOR STORAGE

A Kaspersky Anti-Virus for Storage védi a hálózati tároló termékek EMC Celerra családját mindenféle kártékony programok ellen.

A hálózati adattároló rendszerek bármely méretű vállalat alkalmazottai számára gyors és megosztott hozzáférést nyújtanak az információkhoz. Amennyiben azonban a vállalati hálózat védelme nem megfelelő, a megosztott fájlokhoz való hozzáférés számos nemkívánatos következményhez vezethet.
A rendszerben tárolt egyetlen fertőzött fájl a teljes hálózatot veszélyeztetheti, alapvető üzleti, anyagi és hírnévbeli károkat okozva. Ezért elengedhetetlen a hálózati tárolórendszerek

A Kaspersky Anti-Virus for Storage szoftver teljes mértékben kompatibilis az EMC Celerra termékcsaláddal. Szakértői tervezésnek köszönhetően a legmagasabb szintű védelmet nyújtja, a Celerra rendszerekben tárolt fájlokban és archívumokban felismerve és semlegesítve a kártékony programokat. Ezen megoldás segítségével a rendszergazdák úgy konfigurálhatják a rendszert, hogy valós időben, az objektumok mentésekor és módosításakor, illetve igény esetén végzik átvizsgálási feladataikat.

JELLEMZŐK

- Védelem az EMC Celerra adattároló rendszerekhez
- Támogatás Windows Server® 2008 R2-höz
- Hierarchikus tárolófelügyeleti (HSM) rendszerek támogatása
- Fokozott proaktív védelem az új rosszindulatú programokkal szemben
- Valós idejű vírusvédelem
- Fájlok tárhelyének ütemezett átvizsgálása
- Kritikus rendszerterületek ellenőrzése
- A rendszer erőforrásainak optimalizált használata
- Adatok biztonsági mentése a fertőzött fájlok megtisztítását vagy törlését megelőzően
- Skálázhatóság
- VMware Ready tanúsítvány
- Központosított telepítés, kezelés és frissítések a Kaspersky Security Centeren keresztül
- Teljes mértékben illeszkedik a Kaspersky Endpoint Security for Business Platformhoz és egyéb Kaspersky termékekhez
- Alkalmazásistátusz-értesítési rendszer
- Részletes értesítések a hálózat védelmi státuszával kapcsolatban

KASPERSKY MOBILBIZTONSÁG

Teljes körű mobil biztonság a mobileszköz felügyelet (MDM) és a mobileszközök végpont biztonságának ötvözésével.

A mobil eszközmenedzsment (MDM) segítségével a mobileszközök biztonságos konfigurációja könnyen és egyszerűen megoldható, az eszközökre telepített mobil ügynök gondoskodik az aktuális fenyegetések elleni védelemről - és mindez akár az alkalmazottak saját eszközein is megoldható!

A KASPERSKY SECURITY FOR MOBILE RÉSZLETES JELLEMZŐI:

INFORMATIKAI HATÉKONYSÁGI JELLEMZŐK:

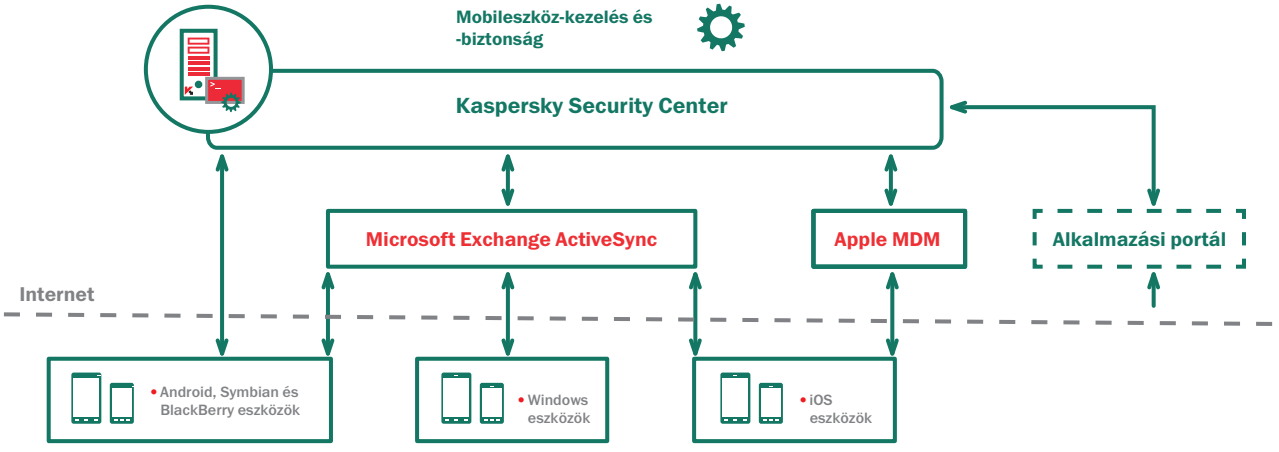
EGYSZERŰ KONFIGURÁCIÓ EGYETLEN KONZOL SEGÍTSÉGÉVEL
Más megoldásoktól eltérően a Kaspersky Lab lehetővé teszi a rendszergazdák számára, hogy egyetlen konzolt használva kezelhessék a mobileszközök, fizikai végpontok, virtuális rendszerek, titkosítási és irányelv-érvényesítési eszközök biztonságát.

SZEMÉLYES ALKALMAZÁSI PORTÁL
A rendszergazdák olyan vállalati portált tesznek közzé, amelyen jóváhagyott alkalmazások linkjei találhatók. A felhasználók kizárólag ezeket az alkalmazásokat használhatják.

OTA (OVER THE AIR) TELEPÍTÉS ÉS KONFIGURÁLÁS
Távolról gondoskodik a telefonok biztonságáról, e-mailben vagy SMS-ben elküldve azon vállalati portál linkjét, ahonnan a rendszergazda által jóváhagyott profilok és alkalmazások letölthetők. Az adatokhoz való hozzáférés csak akkor lesz engedélyezett, ha a felhasználó elfogadja ezeket.

BIZTONSÁGOS KONFIGURÁCIÓ
A hardver és szoftver integritását. Rootolt és jailbroken készülékek érzékelésének engedélyezésével biztosítja. Az egyéb biztonsági beállítások között találjuk többek között a „kamera kikapcsolása” és kötelező jelszóbeállításokat.

MEGFELELŐSÉG ÉS IRÁNYELV ÉRVÉNYESÍTÉSE
Az alkalmazáskontroll lehetővé teszi az eszközökön való alkalmazáshasználat figyelemmel kísérését és támogatja például a „Default deny” (alaphelyzetben elutasít) és „Default allow” (alaphelyzetben engedélyez) beállításokat.



BIZTONSÁGI KOCKÁZATKEZELÉS:

TITKOSÍTÁS
Az adatmozgás teljes lemeztitkosítással (FDE) és fájlszintű adattitkosítással védett, ami konténerekre is alkalmazható.

LOPÁS ELLENI BIZTONSÁGI ZÁR
A rendszergazda távolról törölheti az ellopott készülék teljes vagy részleges tartalmát, GPS segítségével meghatározhatja a készülék helyét, illetve értesítést kérhet arról, ha a készülékből kiveszik a SIM kártyát vagy kicserélik azt.

MOBILESZKÖZÖK KÁRTÉKONY PROGRAMOK ELLENI VÉDELME
A Kaspersky Lab rosszindulatú kártevő programok elleni védelme többrétegű megoldásokat alkalmaz, és többek közt felhő-alapú védelmet ötvöz biztonságos böngészővel és hatékony spam-szűrővel a mobileszközök védelme érdekében.

VÁLLALATI ÉS SZEMÉLYES ADATINTEGRITÁS:

KONTÉNEREK
Az alkalmazottak saját mobileszköz-használatának esetére a vállalati adatok és alkalmazások elkülönített „konténerekbe” helyezhetők.
Ez maximálisan biztosítja a vállalati adatok biztonságát és a személyes tartalmak optimális integritását.

TÁVOLI ADATBIZTONSÁGI ESZKÖZÖK
Az elveszett készülék távolról, a „Remote Lock” funkcióval blokkolható. A készüléken elkülönített konténerben található vállalati adatok biztosíthatók, titkosíthatók, távolról kezelhetők és törölhetők, a készüléken levő személyes adatoktól függetlenül.

TÖKÉLETES A „HASZNÁLD A SAJÁT ESZKÖZÖD (BYOD)” KEZDEMÉNYEZÉSEK TÁMOGATÁSÁRA

Számos alkalmazott saját eszközét használja személyes és vállalati feladatok végrehajtására egyaránt. Manapság számos cégnél bevett szokás, hogy az alkalmazottak saját maguk választják ki és vásárolják meg a nekik tetsző okostelefont vagy táblagépet, majd a cég IT részlege gondoskodik az e-mail fiókok és vállalati hozzáférések feltelepítéséről és beállításáról.

A BYOD megoldás a cégek szempontjából költséghatékony és emeli a termelékenységet is, azonban a jelentős biztonsági kockázatokat hordoz. A nem megfelelően védett és személyes adatokkal kevert céges információk jelentős visszaélésekre adnak lehetőséget. Az eszközöket gyakran az alkalmazottak családtagjai is használják, akik sokszor nincsenek tekintettel az adatvédelem fontosságára. Sőt, nem ritka a rootolt vagy jailbroken eszköz sem.

A Kaspersky Security for Mobile ezekre a problémákra nyújt megoldást, lehetővé téve az okostelefonok és táblagépek biztonságos konfigurációját ugyanazon konzolon keresztül, mint amit a hálózati biztonság beállításához használunk. A rendszergazdák biztosak lehetnek abban, hogy a felhasználók eszközeinek konfigurálása a megfelelő beállításokkal történik, és az adatok és információk a készülékek elvesztése, lopása vagy jogosulatlan használata esetén is védettek.

KASPERSKY RENDSZERFELÜGYELET

A Kaspersky rendszerfelügyelet bemutatása. A megoldás lényege, hogy azonos kódban írt, egy konzolról kezelhető, egymással hatékonyan együttműködő IT eszközöket és alkalmazásokat kínál, egy csomagban. Az eredmény egy olyan platform, amely az ügyfelek által keresett

A KÜLÖNBÖZŐ, ELTÉRŐ IT ALKALMAZÁSOK KOMPLEX RENDSZEREKET EREDMÉNYEZNEK - ÉS A KOMPLEXITÁS A BIZTONSÁG LEGFŐBB ELLENSÉGE.

Felesleges idő- és energiaráfordítás nélkül
A Kaspersky rendszerfelügyeleti megoldással megtakarítható az idő és erőfeszítés, amelyekkel új, illetve meglevő felhasználók részére egyenként kell telepíteni az egyes rendszereket. A rendszerkezelő (system provisioning) technológia segítségével központi helyről lehet lemezképeket létrehozni, kezelni és az egyes felhasználókhoz telepíteni.

A biztonság növelése
A rendszergazdák beszámolói szerint napi munkájuk jelentős részét az teszi ki, hogy gondoskodjanak a rendszereken telepített javítócsomagok frissítéséről. A Kaspersky segít csökkenteni a rendszer összetettségét, azonosítja a kihasználható biztonsági réseket, így eldönthetjük, mely javításokat lehet a munkaidő utánra halasztani.
A feladatok ezen rangsorolása segít a rendszergazdáknak munkanapjuk ütemezésében és a magasabb fokú rendszerbiztonság elérésében.

Hatékony munkavégzés
A rendszergazdák távolról is telepíthetnek képfájlokat, frissítéseket, javítócsomagokat és alkalmazásokat. Ha egy felhasználó hibát észlel, az IT részleg távolról is hozzáfér a gépéhez és a problémákat el tudja hárítani. A rendszergazdának tehát nem kell időt pazarolnia arra, hogy a felhasználókat személyesen felkeresse vagy telefonon keresztül hosszasan magyarázva próbálja elhárítani a hibákat.

Ezek a szolgáltatások - egyebek mellett - a Kaspersky Systems Management részét képzik, és a Kaspersky Security Center adminisztrátori konzolján keresztül érhetők el. Mivel az egyes eszközöknek nincs külön, saját konzoljuk, a parancsok konzisztensek és intuitívak, alkalmazásukhoz nem szükséges külön tréning.

RENDSZERFELÜGYELETI JELLEMZŐK:

OPERÁCIÓS RENDSZEREK ÉS ALKALMAZÁSOK JOGOSULTSÁG KIOSZTÁSA
Rendszerképek egyszerű létrehozása, tárolása, klónozása és telepítése egy központi helyről. A rendszerek problémamentes és optimális biztonsági beállításokkal való átadása a felhasználóknak. Az eszköz alkalmas a Microsoft Windows 8 operációs rendszerre való migrációhoz.

BIZTONSÁGI RÉSEK RANGSOROLÁSA
Egyetlen kattintással a rendszer megvizsgálja a hardvert és szoftvert, és összeveti számos, biztonsági réseket tartalmazó adatbázissal, így fontossági sorrendet állíthatunk fel, hogy melyek azok a biztonsági rések, amelyek azonnali beavatkozást igényelnek, és melyek azok, amelyek megoldását későbbre hagyhatjuk.

TÁVOLI, RUGALMAS SZOFTVERTELEPÍTÉS
Hálózati terhelés minimumra csökkentése kézi vagy ütemezett telepítésekkel.

TÁVOLI ÜGYNÖKALKALMAZÁSOK
Egy távoli irodában vagy leányvállalatnál található munkaállomást kijelölhetünk központi frissítési ügynöknek. Ezáltal sávszélességet takarítunk meg, mivel elegendő egyetlen frissítést elküldeni a távoli irodába - és a helyi, kijelölt munkaállomást használhatjuk a frissítések kiosztásához az adott helyszínen.

WAKE-ON-LAN TECHNOLÓGIA TÁMOGATÁSA
Munkaidő utáni telepítések vagy hibaelhárítás céljából a Kaspersky Systems Management segítségével a munkaállomások távolról is üzembe helyezhetők.

HIBAELHÁRÍTÁSI ESZKÖZÖK
Távolról és biztonságosan kapcsolódni az ügyfél rendszeréhez - mindig ugyanarról az adminisztrátori konzolról.

MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS) TÁMOGATÁS
A Kaspersky Systems Management rendszeresen szinkronizálja az elérhető frissítéseket és javításokat a szerverekkel - többek között a Microsoft Windows Update-tel -, azokat a Windows Update Services útján letölti és hatékonyan kiosztja.

HÁLÓZATI BELÉPTETÉS-ELLENŐRZÉS (NAC)
A hálózati beléptetés-ellenőrzés (NAC) lehetővé teszi, hogy a hálózatra „látogatói” szabályokat állítsunk be. A vendégkészülékek (például mobilkészülékek) felismerése automatikusan megtörténik, és a rendszer átirányítja őket egy olyan céges portálra, ahol a megfelelő jogosultságok birtokában az általunk kijelölt erőforrásokhoz férhetnek hozzá.

HARDVER ÉS SZOFTVER NYILVÁNTARTÁS
A rendszer automatikusan felismeri és nyilvántartja a PC-ket, merevlemezeket, sőt az eltávolítható eszközöket is. Új eszköz csatlakoztatása esetén a rendszer azonnal értesítést küld a rendszergazdának. A funkció segítségével a rendszergazda folyamatosan nyomon követheti a hálózaton üzemelő hardverek állapotát és használatát.

SZOFTVERLICENC KIADÁSA ÉS ELLENŐRZÉSE
A Kaspersky Systems Management pontos tájékoztatást ad arról, milyen szoftvereket használnak az adott környezetben. Ezáltal lehetőségünk van a licencköltségek beállítására és a szabályszegő felhasználók azonosítására. A Kaspersky Lab végpontellenőrző eszközeivel történő telepítés esetén a használat a jóváhagyott alkalmazásokra és verziókra korlátozható - és korlátozhatja az adott időpontban használatban levő licencek számát.

KASPERSKY SECURITY FOR FILE SERVER

A Kaspersky Security for File Server valamennyi kártékony programtól megbízhatóan védi a Microsoft® Windows®, Novell NetWare és Linux szervereket.

A megosztott fájltárolás esetében a vírusok elleni védelem elengedhetetlen, mivel a szerveren található egyetlen fertőzött fájl az erőforrások valamennyi felhasználójának munkaállomását megfertőzheti. A fájlszerver megfelelő védelme nem csak a felhasználók és adataik védelmét biztosítja, hanem a fájlok biztonsági másolatába beférkőző kártékony programok veszélyét is kiküszöböli, ami különben sorozatos fertőzéseket és egyéb baleseteket okozhat.

TERMÉKJELLEMZŐK*

- Támogatás a Microsoft® Windows® és Linux platformokhoz.
- A rendszer erőforrásainak optimalizált használata
- Hierarchikus tárolófelügyeleti (HSM) rendszerek támogatása
- A terminálszerverek és kiszolgálófürtök védelme
- VMware Ready tanúsítvány
- NSS fájlrendszer-támogatás
- Díjmentes BSD támogatás

JELLEMZŐK

- Windows® (többek között Windows Server® 2008 R2), Linux (többek között Samba) és a Novell NetWare fájlszerverek védelme
- Fokozott proaktív védelem az új rosszindulatú programokkal szemben
- Valós idejű vírusvédelem
- Aktív fertőzések kezelése
- Fájlok tárhelyének ütemezett átvizsgálása
- Kritikus rendszerterületek ellenőrzése
- Fertőzött munkaállomások elszigetelése
- Skálázhatóság
- Adatok biztonsági mentése a fertőzött fájlok megtisztítását vagy törlését megelőzően
- Központosított telepítés, kezelés és frissítések
- Telepítési és felügyeleti módszerek választéka
- Átvizsgálási és információs biztonsági incidens válaszhelyzetek rugalmas rendszere
- Alkalmazásistátusz-értesítési rendszer
- Részletes értesítések a hálózat védelmi státuszával kapcsolatban

ALKALMAZÁSOK

- Kaspersky Anti-Virus for Windows® ISA Server vállalati kiadás
- Kaspersky vírusirtó Linux fájlszerverhez
- Kaspersky vállalati végpontbiztonság Windows® rendszerhez
- Kaspersky vírusirtó Novell NetWare-hez
- Kaspersky Security Center

*A termékjellemzők a felhasznált alkotóelemek kombinációjának függvényében változhatnak. Az egyes alkotóelemek leírásával kapcsolatos további információért lásd a www.kaspersky.com, vagy a www.kaspersky.hu oldalt.

KASPERSKY SECURITY LEVELEZŐSZERVERHEZ

A Kaspersky levelezőszerverekhez készült védelmi megoldásai a levelező-szerverek és a csoportszoftver-szerverek számára is védelmet nyújt a kártékony programokkal és a levélszeméttel szemben.

A termék olyan alkalmazásokat tartalmaz, amelyek valamennyi népszerű szerver, többek között Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim és CommuniGate Pro levélforgalmát védik. A megoldás külön elektronikuslevél-átjáró beállítására is alkalmas.

TERMÉKJELLEMZŐK*

LEVÉLSZERVER VÉDELEM
Kártékony programok elleni védelem és a levélforgalom spamvédelme valamennyi népszerű levelezőrendszerhez.

A RENDSZER ERŐFORRÁSAINAK OPTIMALIZÁLÁSA
Új antivírus motor, szerver erőforrások terhelésének kiegyenlítése és a vizsgálati kivételek alkalmazása együttesen a rendszer terhelését csökkentik.

KSN INTEGRÁCIÓ A SPAMVÉDELEM ÉRDEKÉBEN
A spam felismerési aránya növekszik a Kaspersky Lab felhőalapú fenyegetésazonosítási motorjával (KSN) való integrációnak köszönhetően.

FORGALOM JELENTETTE CSÖKKENTETT TERHELÉS
A felhőkompatibilis, intelligens spamszűrés jelentősen csökkenti a forgalom jelentette terhelést.

JELLEMZŐK

- Levelezőszerverek integrált védelme mindenféle rosszindulatú programmal szemben
- Hatékony spamvédelem
- Valós idejű vírusvédelem
- E-mailek és adatbázisok ütemezett átvizsgálása
- Sendmail, qmail, Postfix, Exim és CommuniGate Pro levelezőszerverek védelme
- Üzenetek, adatbázisok és egyéb objektumok átvizsgálása Lotus® Domino® szervereken
- Valamennyi üzenet átvizsgálása Microsoft® Exchange szerveren, beleértve a nyilvános mappákat
- Üzenetek szűrése a csatolmány típusa alapján
- Skálázhatóság
- Támogatás a Microsoft® Exchange Server 2007 klaszterekhez és DAG for Microsoft® Exchange Server 2010-hez
- Adatok biztonsági mentése a fertőzött fájlok megtisztítását vagy törlését megelőzően
- A fertőzött tárgyak elszigetelése
- Ismételt üzenetátvizsgálás megszüntetése
- Kényelmes eszközök a telepítéshez, kezeléshez és frissítésekhez
- Részletes értesítések a védelmi státuszról
- Átvizsgálási és információs biztonsági incidens válaszhelyzetek rugalmas rendszere
- Alkalmazásistátusz-értesítési rendszer

APPLICATIONS

- Kaspersky Security a Microsoft® Exchange szerverekhez
- Kaspersky vírusirtó a Lotus® Domino®-hoz
- Kaspersky Security a Microsoft® Exchange Server 2003-hoz
- Kaspersky Security a Linux levelezőszerverhez

*A termékjellemzők a felhasznált alkotóelemek kombinációjának függvényében változhatnak. Az egyes alkotóelemek leírásával kapcsolatos további információért lásd a www.kaspersky.com, vagy a www.kaspersky.hu oldalt.

KASPERSKY SECURITY FOR VIRTUALIZATION

A Kaspersky Security for Virtualization – amelyet a virtualizált informatikai környezetek egyedi követelményeihez terveztek — kártékony programok ellen díjnyertes védelmet nyújt a virtualizált szerverek, desktopok és adatközpontok számára.

A Kaspersky Security for Virtualization egy kártékony programok elleni ügynök nélküli megoldás, amelynek segítségével még hatékonyabban védelmezheti virtualizált infrastruktúráját — jobb teljesítménnyel és kisebb hatással a virtualizációs sűrűségre. Az alkalmazás telepítése egyszerű, és fejlett felügyeleti jellemzőkkel rendelkezik, amelyek a biztonsági feladatok széles körét leegyszerűsítik — a fizikai és virtuális informatikai eszközökön egyaránt.

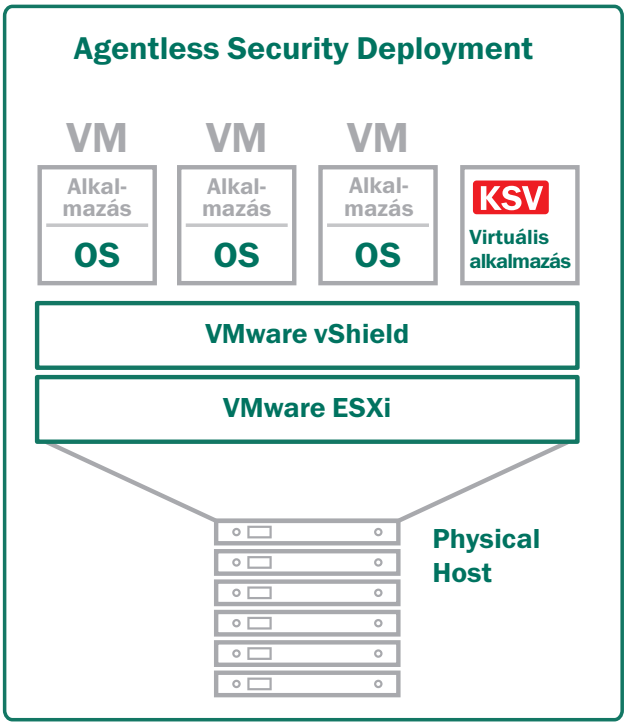
VÉDELEMMEL ÉS TELJESÍTMÉNNYEL

- Központosított biztonság. A Kaspersky Security for Virtualization olyan virtuális alkalmazás, amely a VMware vShield Endpoint-hoz csatlakozik, és a kártékony programok átvizsgálásával foglalkozik. Minden egyes fizikai hosztot egyetlen, központosított antivírus motorral és adatbázissal lát el.

- Fejlett antivírus motor. A Kaspersky kártékony programok elleni díjnyertes technológiája — a Kaspersky által kínált, az iparágban vezető frissítési gyakorisággal — segít az új vírusok elleni védelemben. A heurisztikus elemző felveszi a harcot a sokféle alakú kártékony programok ellen.

- Automatikus védelem. Az új virtuális gépek automatikusan kártékony programok elleni védelemmel vannak ellátva — a biztonsági rések és a nem megfelelő konfigurációk kiküszöbölésének elősegítése érdekében. Bármely virtuális gépet minden esetben a legújabb aláírás alapú adatbázis véd, attól függetlenül, hogy a virtuális gép korábban csatlakozott-e az internethez.

- Nagyobb sűrűségű virtualizáció. Mivel a Kaspersky Security for Virtualization ügynök nélküli megoldás, segít a „frissítési hullámok” és a „átvizsgálási hullámok” kiküszöbölésében, csökkenti a teljesítményre gyakorolt hatást és a biztonsági réseket célozza, amelyeket egyes ügynök alapú termékek okozhatnak.



A Kaspersky Security for Virtualization ügynök nélküli vírusirtást nyújt VMware telepítésekhez

A RENDSZERFELÜGYELETI MEGOLDÁS JELLEMZŐI:

EGYETLEN KEZELŐKONZOL

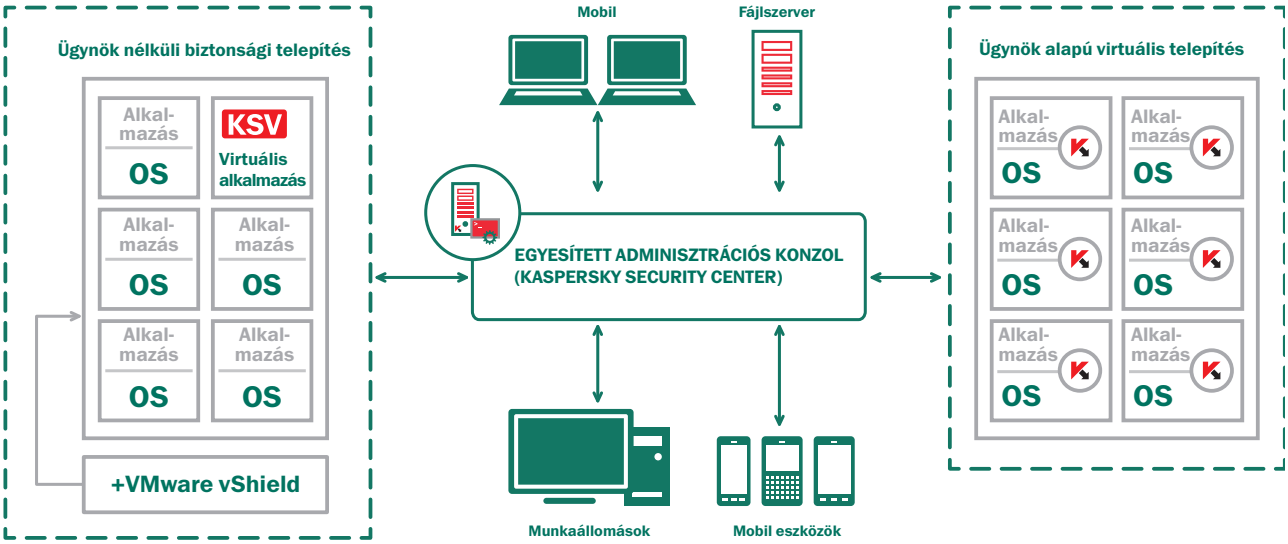
A Kaspersky Security Center — amely további költség nélkül hozzáférhető — egyetlen kezelőkonzol, amely lehetővé teszi a virtuális gépek, fizikai gépek és mobileszközök biztonságának felügyeletét.

VMWARE VMOTION TÁMOGATÁS

A VMware vMotion-t teljes mértékben támogató Kaspersky Security for Virtualization biztosítja, hogy a védelem nem szakad meg egy munkateher egyik ESXi hosztról a másikra való áthelyezésénél. Amennyiben az új hoszt rendelkezik a szükséges licenccel, a védelem követi a munkaterhet, és valamennyi biztonsági beállítás változatlan marad.

A VMWARE VCENTERREL EGYSÉGBEN.

A Kaspersky Security for Virtualization a vCentertől kap információt a virtuális gépekről — beleértve valamennyi virtuális gép listáját és a kapcsolódó paramétereket. Amellett, hogy az informatikai csapat számára nagyobb átláthatóságot jelent, a VCenterrel való integráció biztosítja az automatikus védelmet új virtuális gép konfigurálása esetén.



KSV Kaspersky Security for Virtualization

Kaspersky Lab biztonsági megoldás

KASPERSKY SECURITY FOR INTERNET GATEWAY

A KASPERSKY SECURITY for Internet Gateway biztonságos internet hozzáférést biztosít a szervezet valamennyi alkalmazottjának.

A Kaspersky Security for Internet Gateway támogatja a Windows és Linux platformokon működő legnépszerűbb internetes átjárókat. A HTTP, HTTPS, FTP, POP3 és SMTP protokollokon futó köztudottan veszélyes és esetlegesen veszélyes programokat automatikusan felismerik az adatáramban. Az optimalizációs technológiának, a skálázhatóságnak és a legújabb platformok támogatásának köszönhetően ideális termék óriási forgalmat bonyolító vállalatok számára.

TERMÉKJELLEMZŐK*

- Microsoft® Forefront® TMG védelem
- Irányelv kezelési és konfigurációs eszközök széles választéka
- VPN-kapcsolatok átvizsgálása
- E-mail forgalom védelme (POP3 és SMTP protokollokon keresztül)
- A nyilvános szervekről érkező HTTP és FTP forgalom átvizsgálása
- VMware Ready tanúsítvány

JELLEMZŐK

- A HTTP, HTTPS, FTP, POP3 és SMTP protokollokon keresztül érkező internetes forgalom valós idejű átvizsgálása
- Integrált védelem mindenféle rosszindulatú program ellen
- Támogatás Squid, Blue Coat és Cisco® proxy szerverekhez
- Háttértárolás
- Szerver processzorok kiegyensúlyozott terhelése
- Skálázhatóság
- Kényelmes eszközök a telepítéshez, kezeléshez és frissítésekhez
- Átvizsgálási és információs biztonsági incidens válaszhelyzetek rugalmas rendszere
- Részletes értesítések a hálózat védelmi státuszával kapcsolatban

ALKALMAZÁSOK

- Kaspersky Anti-Virus for Microsoft® ISA Server and Forefront® TMG hagyományos kiadás
- Kaspersky Anti-Virus for Microsoft® ISA Server vállalati kiadás
- Kaspersky Anti-Virus for Proxy Server

*A termékjellemzők a felhasznált komponensek kombinációjának függvényében változhatnak. Az egyes alkotóelemek leírásával kapcsolatos további információért lásd a www.kaspersky.com, vagy a www.kaspersky.hu oldalt.

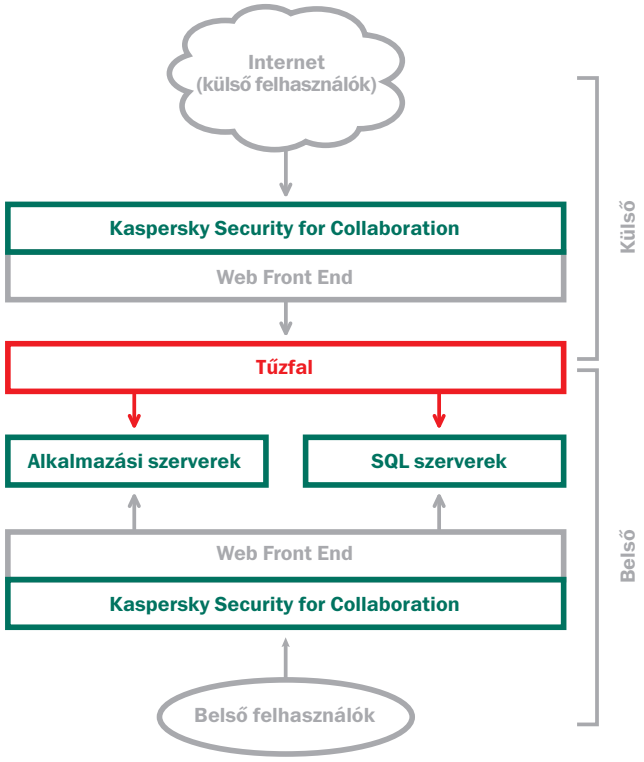
KASPERSKY SECURITY FOR COLLABORATION

A Kaspersky Security for Collaboration a legújabb védelmi technológiákat alkalmazza az együttműködési platformon, egyszerű kezelés és a kártékony programok nagy felismerési arányának ötvözetével.

A Kaspersky Security for Collaboration a Kaspersky díjnyertes antivírus motorjának segítségével nyújt védelmet a Microsoft® SharePoint® környezetek számára. A kártékony programok felismerésére alkotott díjnyertes technológiának köszönhetően a termék képes egyetlen szerver vagy egész SharePoint farmok védelmére — míg tartalma és fájlszűrő képességei segítik a nem megfelelő tartalom tárolásának megelőzését.

JELLEMZŐK

- Az innovatív felismerési technológia a feltöltéseknél és letöltéseknél valós időben azonosítja és blokkolja a kártékony programokat
- A végfelhasználókat megakadályozza abban, hogy meghatározott típusú (pl. zenéket, videókat, exe fájlokat) vagy nem megfelelő tartalmú fájlokat tároljanak
- A nemzetközi kezelési beállítások valamennyi védett szerveren egyetlen kezelőpultról konfigurálhatók
- Egyszerű, intuitív felügyelet — különleges képzést nem igényel
- Active Directory beállításokkal és felhasználó-azonosítással való integráció
- A részletes naplók és a módosított fájlok biztonsági mentése segít a rendszergazdáknak a szabályszegési és biztonsági kérdések kezelésében
- Részletes, rugalmas jelentéskészítési lehetőség



KASPERSKY SMALL OFFICE SECURITY

A Kaspersky Small Office Security-t kifejezetten kisvállalkozások számára tervezték. Megfizethető áron nyújt világszínvonalú PC- és szervervédelmet, mely gyorsan és egyszerűen telepíthető, konfigurálható és használható.

A teljes vállalati hálózat menedzselhető egyetlen számítógépről, elvégezve a zavartalan vállalati ügymenethez szükséges összes adatbiztonságot érintő feladatot az íróasztal elhagyása nélkül. A Kaspersky Small Office Security gondoskodik a hálózat védelméről, így Ön a vállalat sikeres üzletmenetére koncentrálhat. Tartsa biztonságban digitális munkaterületét, a vállalat lehető legmegfelelőbb védelmével.

JELLEMZŐK

- Valós idejű védelem vírusok, kémprogramok, trójai programok és egyebek ellen
- Az alkalmazottak honlapokhoz, alkalmazásokhoz, játékokhoz és közösségi oldalakhoz való hozzáférésének korlátozása
- A vállalati adatok teljes körű védelme ütemezett, automatikus biztonsági háttérmentésekkel
- Adatok tárolása olyan titkosított adatszéfekben, melyek biztonságosan továbbíthatók e-mailen keresztül vagy USB háttértáron
- Nehezen feltörhető jelszavak létrehozása és tárolása Ön és alkalmazottai számára*
- Maximális rendszerteljesítmény biztosítása gyakori frissítésekkel és diszkrét működéssel
- Fejlett technológiák a hekkertámadások azonnali blokkolására
- A vállalati informatikai hálózat, beleértve a WiFi-t, biztonságának növelési eszközei
- Fájlzúzó az érzékeny adatok törlésére, így megakadályozható azok visszanyerése vagy ellopása

ADMINISZTRÁCIÓ

- Központosított hálózati biztonság kezelés egyetlen számítógépről
- Egyszerű, intuitív interfész
- Könnyű kezelhetőség, a nagyobb hálózati biztonság biztosítása céljából
- Internethasználati sémák kezelése

ALKALMAZÁSOK

A Kaspersky Small Office Security csomag által támogatott platformok/operációs rendszerek:

- Microsoft® Windows® (beleértve Microsoft® Windows® 7)
- Windows® szerverek (többek között Windows Server® 2008 R2)

Kaspersky Lab ZAO, Moszkva, Oroszország
www.kaspersky.com

Az internetes biztonsággal kapcsolatos információ:
www.securelist.com

Viszonteladó keresése az Ön közelében:
www.kaspersky.com/buyoffline

KASPERSKY lab