KASPERSKY SECURITY FOR COLLABORATION

Védelem és szabályozás a kollaborációs platformok számára, ideértve a SharePoint-parkokat is.

A fájlok és adatok megosztásához használt platform ideális közvetítőrendszerként szolgálhat a veszélyes rosszindulatú programok és egyéb IT-fenyegetések számára.
A biztonságos és problémamentes megosztott munkakörnyezet érdekében a Kaspersky Lab kifejlesztett egy megoldást, mely az egyszerű felügyelet mellett valós idejű, prémium szintű védelmet biztosít a rosszindulatú programok támadásai és a bizalmas adatok kiszivárgása ellen.

- Díjnyertes kártékony programok elleni program
- Bizalmas adatok „keresése és védelme”
- Adathozzáférés-felügyelet
- Felhőalapú, valós idejű védelem – Kaspersky Security Network
- Fájl- és tartalomszűrés
- Adathalászat elleni védelem
- Biztonsági mentés és tárolás
- Centralizált, rugalmas felügyelet
- Intuitív adminisztrációs konzol

FŐBB JELLEMZŐK

TELJES VÉDELEM A SHAREPOINT PLATFORM SZÁMÁRA.

Ha Microsoft SharePoint kiszolgálót használ, akkor tudja, hogy mivel minden tartalom egy SQL-adatbázisban tárolódik, a hagyományos végpontvédelmi megoldások nem elegendők. A Kaspersky Security for Collaboration díjnyertes, fejlett rosszindulatú programok elleni védelmet használ a SharePoint-park és a felhasználók védelme érdekében. Hatékony védelem az ismert, ismeretlen és speciális fenyegetések ellen a felhőalapú Kaspersky Security Network segítségével, míg az adathalászat elleni technológia a kollaboratív adatok ellen irányuló, webalapú fenyegetésekkel szemben nyújt védelmet.

A BIZALMAS ADATOK KISZIVÁRGÁSÁNAK MEGAKADÁLYOZÁSA.

A bizalmas adatok áramlásának felügyelete és védelme érdekében első lépésként az adatokat kell azonosítani. Az előre telepített vagy egyedi szótárak és adatkategóriák használatával a Kaspersky Security for Collaboration a SharePoint kiszolgálókon elhelyezett minden dokumentumban szóról szóra, kifejezésről kifejezésre ellenőrzi az érzékeny információkat. A személyes és kártyaadatok esetében kifejezetten fontos a megfelelő védelem és felügyelet, míg a struktúra-alapú keresések az olyan érzékeny dokumentumokat is azonosítják, mint az ügyfél adatbázisai.

KOMMUNIKÁCIÓS IRÁNYELVEK VÉGREHAJTÁSA.

A tartalom- és fájlszűrési funkciók elősegítik a kommunikációs irányelvek és szabványok betartását, azonosítják és blokkolják a nem megfelelő tartalmakat, emellett pedig megakadályozzák, hogy a helytelen fájlok és fájlformátumok értékes helyet foglaljanak a rendszereken.

EGYSZERŰ KEZELÉS.

A teljes kiszolgálópark biztonságát egyetlen központosított, intuitív felületről vezérelheti. Az adminisztráció gyors és pofonegyszerű, így külön képzést nem igényel.

VÍRUSOK ELLENI VÉDELEM

- **Ellenőrzés hozzáféréskor** – a fájlokat az alkalmazás fel- és letöltés közben, valós időben ellenőrzi.
- **Ellenőrzés a háttérben** – a program a rosszindulatú programok legújabb aláírásai alapján rendszeresen vizsgálja a kiszolgálón tárolt fájlokat.
- **Integráció a Kaspersky Security Network felhőalkalmazással** – valós idejű, felhőalapú védelem még a nulladik napi fenyegetésekkel szemben is.

TÁMOGATJA A VÁLLALAT KOMMUNIKÁCIÓS SZABÁLYAIT

- **Fájlszűrés** – segít a dokumentumtárolási szabályok betartásában és a tárolóeszközök igénybevételének csökkentésében. A valós fájlformátumok elemzésével az alkalmazás a kiterjesztés nevétől függetlenül biztosítja, hogy a tiltott fájlkiterjesztések használatának elkerülésével a felhasználók ne kerülhessék meg a biztonsági szabályokat.
- **Wikioldalak és blogok védelme** – védelmet biztosít minden SharePoint gyűjtemény, például a wikioldalak és blogok számára.
- **Tartalomszűrés** – Az alkalmazás fájltípustól függetlenül képes a nemkívánatos tartalmak tárolásának megakadályozására. A program minden fájl tartalmát kulcsszavak alapján ellenőrzi. Az ügyfelek emellett saját, egyedi szótárakat is létrehozhatnak a tartalomszűréshez.

BIZALMAS ADATOK KISZIVÁRGÁSÁNAK MEGAKADÁLYOZÁSA

- **Bizalmas információk keresése a dokumentumokban** – A Kaspersky Security for Collaboration a SharePoint kiszolgálókra letöltött minden dokumentumban ellenőrzi a bizalmas információkat.
  A megoldás olyan modulokat integrál, melyek bizonyos adattípusokat azonosítanak és leellenőrzik, hogy azok megfelelnek-e a jogi normáknak – például személyes adatok (olyan jogszabályok által meghatározva, mint a HIPAA vagy a 95/46/EK EU irányelv) vagy PCI DSS szabvány adatok (Payment Card Industry Data Security Standard).
  Az adatok ellenőrzése beépített, rendszeresen frissített tematikus és testre szabott szótárak alapján történik. A tematikus szótárak többek között „Pénzügyi”, „Adminisztratív dokumentumok” és „Megalázó és sértő nyelv” kategóriákat tartalmaznak.
- **Strukturált adatkeresés** – ha egy üzenetben speciális struktúrába rendezett adatok találhatók, a rendszer potenciálisan bizalmasként kezeli azokat, így biztosítva az olyan érzékeny adatok védelmét, mint az ügyfelek összetett adatbázisai.

RUGALMAS FELÜGYELET

- **Egyszerű felügyelet** – egyetlen konzolról akár egy egész kiszolgálópark is felügyelhető. Egyetlen intuitív kezelőfelület tartalmazza az összes gyakran használt adminisztratív forgatókönyvet.
- **Egy irányítópult** – az egyszerűen használható irányítópult valós idejű hozzáférést biztosít a termékek aktuális állapotához, az adatbázis-verziókhoz és a licencállapothoz az összes védett kiszolgálóra vonatkozóan.
- **Módosított fájlok biztonsági mentése** – probléma esetén lehetőség van az eredeti fájlok visszaállítására, és a módosított fájlokról készült részletes biztonsági mentés a kivizsgálásokhoz is felhasználható.
- **Active Directory®** integráció – az Active Directory-felhasználók hitelesítéséről is gondoskodik.

RENDSZERKÖVETELMÉNYEK

SharePoint kiszolgálók

- Microsoft SharePoint 2010;
- Microsoft SharePoint 2013.

Operációs rendszer (a megoldás telepítéséhez)

SharePoint Server 2010 esetén:

- Windows Server 2008 ×64/ 2008 R2/2012 R2.

SharePoint Server 2013 esetén:

- Windows Server 2008 R2 ×64 SP1/2012 ×64/2012 R2

A rendszerkövetelmények teljes listáját a kaspersky.com címen találja meg

A vásárlás módja

A Kaspersky Security for Collaboration a Kaspersky Total Security for Business alkalmazás részeként vagy különálló, célzott megoldásként vásárolható meg

Megjegyzés! A termék megvásárlásakor a bizalmas adatok kiszivárgását megakadályozó opció külön vásárolható meg.

Kaspersky Security for Collaboration/0.3 verzió/2015. január/Globális

KASPERSKY lab