

# Endpoint Protector 2008™

Az Ön érzékeny adatai csak annyira vannak biztonságban, mint a hálózati végpontok.

Az Endpoint Protector 2008 kiegészíti a mintákon alapuló biztonsági megoldásokat, valamint támogatja a szabály alapú megközelítést, hogy kikényszerítse a szabályok használatát a hálózati végpontokban található eszközökön. Egy olyan világban, ahol a hordozható eszközök egyre növekvő mértékben formálják életünket, az Endpoint Protector 2008 úgy lett kialakítva, hogy fenntartsa a termelékenységet, mindeközben pedig életünket, munkánkat kényelmesebbé és biztonságossá tegye. A kivétel-lista alapú megközelítés kiválasztott felhasználók és csoportok számára lehetővé teszi az engedélyezett eszközök használatát. A munkatársak így produktívak maradnak, de megoldott annak ellenőrzése, hogy milyen eszközöket használhatnak és milyen adatokat hordozhatnak a különféle eszközök között. Az Endpoint Protector 2008 drasztikus mértékben csökkenti a belső fenyegetések kockázatát. Csökken a lehetősége a bizalmas adatok szivárgásának, ellopásának, sérülésének és egyéb módon történő kompromitálásának.

## Szabályozott eszköz típusok:

- USB Flash
- Wireless USB
- Memória kártyák (SD, MMC, CF, etc.)
- Kártya olvasók (belső és külső)
- ZIP meghajtó
- Floppy
- CD/DVD-lejátszó/író (belső és külső)
- Digitális kamera
- Okostelefonok/ PDA/kézi eszközök
- iPods
- külső HDD
- FireWire eszközök
- MP3 lejátszó/ Média lejátszó eszközök
- Biometrikus eszközök

Az Endpoint Protector 2008 úgy viselkedik, mint egy PC és a szabályozott eszköz közötti tűzfal

Az Endpoint Protector 2008 lehetővé teszi a cégek számára, hogy jobban megfeleljenek a hordozható eszközökre vonatkozó szabályozásoknak és megakadályozzák az adatszivárgást.



Titkosítsa az adatait a végpontokban Trusted Device-szal!



## Végpont szintű biztonság munkaállomások és laptopok számára

Védje meg számítógépeit azoktól a fenyegetésektől, melyeket a hordozható adattárolók és más eszközök, mint például az USB memóriák, MP3 lejátszók, belső CD/DVD meghajtók, vagy akár a floppy eszközök rejtenek, amelyek szándékosan vagy véletlenül járulnak hozzá az adatlopáshoz, adatvesztéshez és vírusok vagy kártevők által okozott fertőzéshez.

## Központosított web alapú eszköz menedzsment

A hálózati adminisztrátorok központilag menedzselhetik és engedélyezhetik az eszközök használatát. Az Endpoint Protector 2008 úgy lett kialakítva, hogy találkozzon, mind a menedzsment, mind a biztonságért felelős munkatársak igényeivel. A menedzsment felületen elérjük a valós idejű információkat, grafikonokat, és jelentéseket készíthetünk a szervezeten belül használt eszközökről és az adatok mozgásáról.

## Felügyelje az adatáramlást: fájl követés, fájl árnyékolás

A termék a hálózati végpontoknál történő információ áramlások teljes körű rögzítésével támogatja az adatfolyamok és az adatszivárgás hatásainak vizsgálatát. A fájl követés segítségével nyomon követhetjük az engedélyezett adattároló eszközökre történt adatmásolásokat. A fájl árnyékolás segítségével mindenről másolat készül még akkor is, ha olyan fájlokat törölünk, amelyeket hálózati tároló szerverrel történő kapcsolatban használt a felügyelt eszköz.

## Eszköz aktivitási napló – Audit napló

Az eszközök működését nyomon követő napló készül az összes számítógéphez és eszközhöz kapcsolódóan. Tárolásra kerülnek az olyan adminisztratív teendők is, mint például az eszközök engedélyezése. A napló teljes körű adatszolgáltatást biztosít későbbi vizsgálatokhoz és ellenőrzésekhez.

## Jelentéskészítő eszközök

Az Endpoint Protector 2008 rendelkezik olyan jelentéskészítő és elemző eszközzel, amely könnyűvé és egyszerűvé teszi az adatok vizsgálatának folyamatát.

## Biztonsági szabályok egyszerű érvényesítése

Az eszközök kezelését megkönnyítik a testreszabható sablonok, melyek felhasználó és csoport jogok definiálását teszik lehetővé. A hálózat egészére vonatkozó kötelező szabályokat is létrehozhatunk, és ki is kényszeríthetjük azokat.

## Hálózati kapcsolat nélküli üzemmód az utazó munkatársaknak

A cég hálózatától gyakran távol lévő számítógépek, például a laptopok, is védettek maradnak! Minden értesítés elküldésre kerül a cég hálózatára történő következő csatlakozásnál.

Kényszerítse ki a biztonsági szabályokat és tudja meg, ki és hogyan használja az adatokat.

### RENDSZER KÖVETELMÉNYEK:

#### Kliens oldalon

- Windows Vista (32 bit)
- Windows XP (SP2) (32 bit)
- Windows 2003 (32 bit)
- Windows 2000 (SP4)
- .Net 2.0 Framework
- Minimálisan 32 MB tárhely

#### Szerver oldalon

Támogatott operációs rendszerek:

- Windows 2003 szerver
- Bármely Linux terjesztés

Támogatott Web szerver:

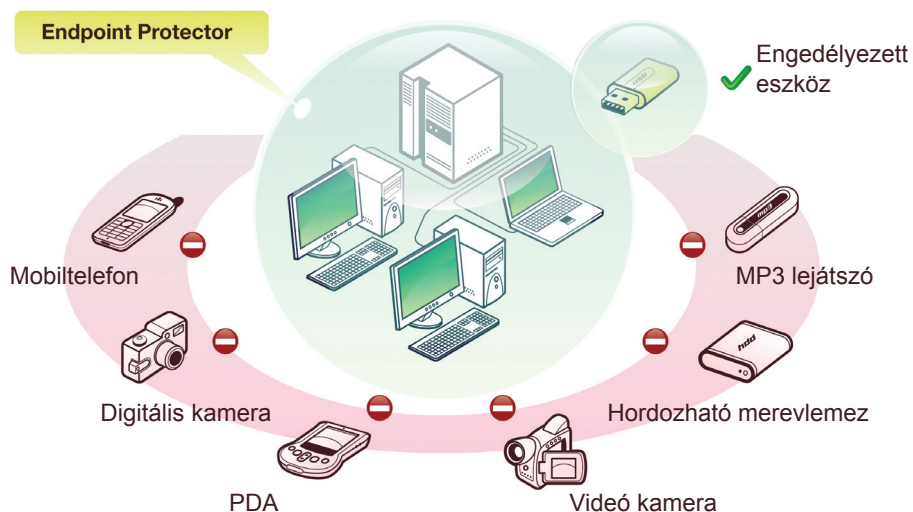
- IIS 6.0
- Apache

Támogatott adatbázisok:

- Microsoft SQL 2005 (Express)

További szerver követelmények:

- MySQL (5, vagy újabb verzió)
- PHP5 SOAP támogatással
- OpenSSL 0.9.8 verzió



Kényelmes telepítés, amely az MSI telepítési mechanizmuson alapul.

Az Endpoint Protector 2008 szerver kompatibilis a különböző szerver platformokkal, biztosítva a gyors és költséghatékony integrációt a már meglévő infrastruktúrába.

Az intuitív web adminisztrációs felület lehetővé teszi a hatékony adminisztrációt.



Az Endpoint Protector 2008 biztonságos, hordozható adattárolókkal és számítógépekkel teli környezetet biztosít. A felhasználó munkavégzése nincs korlátozva, mivel bármely, a védett PC-ken engedélyezett eszköz folyamatosan használható.

#### TrustedDevice / Kikényszerített titkosítás - az utazó adatok védelme

A TrustedDevice technológia biztosítja, hogy a nagyvállalati környezetben az eszközökön lévő adatokat ne csak a védelmi eszköz és a kialakított szabályok védjék, de biztosítva legyen az "utazó adatok" védelme és bizalmassága is. A felhasznált titkosítási módszer biztosítja az elveszett vagy eltulajdonított eszközökön lévő adatok továbbra is bizalmasak maradjanak.

További információk és demó:



**Linux Support Center**

Web: [www.lsc.hu](http://www.lsc.hu)

E-Mail: [endpoint@lsc.hu](mailto:endpoint@lsc.hu)

Tel.: +36-1-341-0457



© Copyright 2004-2008 CoSoSys Ltd. Minden jog fenntartva. A Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin és az Endpoint Protector a CoSoSys SRL regisztrált védjegye. A dokumentumban előforduló egyéb márka és terméknevek az azonosítást szolgálják és jogaikkal tulajdonosaik rendelkeznek.