

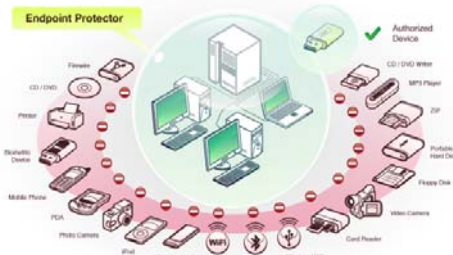


# Endpoint Protector 2009™

## Vállalati Eszköz Ellenőrzés és Adatvesztés megelőzése

Windows XP/Vista/7 Kliens Verzio: 3.0.7.3 Windows 2003/2008 Server Verzio: 3.0.4.1  
Mac OS X Verzio: 1.0.4.4 Linux Server Verzio: 3.0.4.1

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



Az Endpoint Protector 2009 kiegészíti a mintákon alapuló biztonsági megoldásokat, valamint támogatja a szabály alapú megközelítést, hogy kikényszerítse a szabályok használatát a hálózati végpontokban található eszközökön. Az egyedüli megoldás a számítógépek és Mac-ek védelmére. Egy olyan világban, ahol a hordozható eszközök egyre növekvő mértékben formálják életünket, az Endpoint Protector 2009 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 2009 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 Drives (Normál USB Drives, U3, stb.)
- Memória kártyák (SD, MMC, CF, stb.)
- CD/DVD-lejátszó/író (belső és külső)
- Külső HDD
- Floppy
- Kártya olvasók (belső és külső)
- ZIP meghajtó
- Digitális kamera
- Okostelefonok/BlackBerry/PDA/iPods/iPhone
- FireWire eszközök
- MP3 lejátszó/ Média lejátszó eszközök
- Biometrikus eszközök
- Nyomatók
- ExpressCards (SSD)
- Wireless USB

**Az Endpoint Protector 2009 úgy viselkedik, mint egy PC és a szabályozott eszköz közötti tűzfal**

Az Endpoint Protector 2009 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 PC, laptopok / Netbookok számára

Védelem a hordozható eszközök fenyegetései ellen. Megállítja a szándékos vagy véletlenül történő adatlopást, adatvesztést, szivárgást vagy vírusok által okozott fertőzéseket.

### Eszköz menedzsment / Eszköz ellenőrzés

Meghatározza a hálózati eszközök, számítógépek vagy felhasználók jogait.

### Központosított web alapú menedzsment / Műszerfal

A hordozható eszközök központilag menedzselhetők. A web alapú Adminisztratív és jelentéskészítő felület kielégíti mind a menedzsment, mind a biztonságért felelős munkatársak igényeit és valós idejű információkat nyújt a szervezeten belül használt eszközökről, valamint az adatok mozgásáról.

### Fájl követés / Fájl árnyékolás

A fájl követés segítségével nyomon követhetjük az engedélyezett adattároló eszközökre történt adatmásolásokat. A fájl árnyékolás mindenről másolatot készít, még a kitörölt fájlokról is, melyek kapcsolatba kerültek a biztosított eszközökkel.

### Kivétel-lista

Csak az engedélyezett fájlok másolhatók engedélyezett eszközökre. Minden más fájl blokkolva van és a másolási kísérletek jelentésre kerülnek.

### Eszköz aktivitási napló – Audit napló

Az eszközök működését nyomon követő napló készül az összes számítógéphez és eszközhöz kapcsolódóan. Minden eszköz, számítógép vagy felhasználó tevékenysége részletesen van elemzve és tárolva.

### Jelentéskészítés és elemzés

Jelentések, elemzések és grafikonok, melyek egyszerűen teszik a tevékenység vizsgálatát.

### Biztonsági szabályok egyszerű érvényesítése (Active Directory)

Az eszközök kezelését megkönnyítik a testreszabható sablonok, melyek felhasználó és csoport jogok definiálását teszik lehetővé (Active Directory GPOs). A hálózat egészére vonatkozó szabályok is kikényszeríthetők.

### Jelszó nélküli átmeneti üzemmód / Hálózati kapcsolat nélküli üzemmód

A hálózatról lekapcsolt számítógépek védve maradnak. Hogy a produktívitás az úton is fennmaradjon az eszközöket ideiglenesen engedélyezni lehet a Jelszó nélküli átmeneti üzemmód által.

### Endpoint Protector Ügyféli Önvédelem

Olyan számítógépek esetén is védelmet nyújt, melyeken a felhasználók adminisztratív jogokkal rendelkeznek.

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

## RENDSZERER KÖVETELMÉNYEK:

### Kliens oldalon

- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.4+
- .Net 2.0 Framework
- Minimálisan 32 MB tárhely

### Szerver oldalon

Támogatott operációs rendszerek:

- Windows 2003 Server
- Windows 2008 Server
- Debian (\*Ubuntu), Red Hat (Fedora, CentOS), Suse

Támogatott Web szerver:

- IIS 6.0 / 7.0
- Apache

Támogatott adatbázisok:

- Microsoft SQL 2005/2008 (Exp.)
- or MySQL (Version 5 or newer)

További szerver követelmények:

- PHP5 SOAP támogatással
- OpenSSL 0.9.8 verzió

### Címtár

- Active Directory

Kényelmes telepítés, amely az MSI telepítési mechanizmuson alapul.

Az Endpoint Protector 2009 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 2009 biztonságos, hordozható adattárolókkal és számítógépekkel teli környezetet biztosít. A felhasználó munkavégzése nincs korlátozva, mivel bármely, a védett PC-ken engedélyezett eszköz folyamatosan használható.

## Kikényszerített titkosítás - az utazó adatok védelme TrustedDevice által

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.

Több információ vagy ingyenes próbaverzió érdekében látogassa meg a [www.EndpointProtector.com](http://www.EndpointProtector.com) weboldalt.



**CoSoSys Ltd.**

E-Mail: [sales@cososys.com](mailto:sales@cososys.com)

Phone: +40-264-593110

Fax: +40-264-593113

**CoSoSys Security NA**

E-Mail: [sales.us@cososys.com](mailto:sales.us@cososys.com)

Phone: +1-208-850 7563

**CoSoSys Germany**

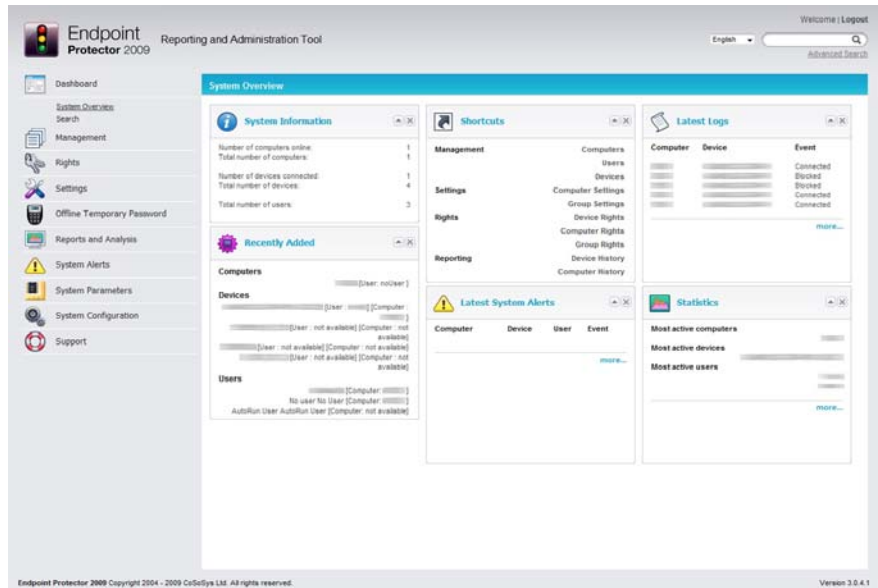
E-Mail: [sales.de@cososys.com](mailto:sales.de@cososys.com)

Phone: +49-7541-978-2627-0

Fax: +49-7541-978-2627-9



© Copyright 2004-2010 CoSoSys Ltd. Minden jog fenntartva. A Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Secure it Easy, TrustedDevices, EasyLock, My Endpoint Protector és az Endpoint Protector a CoSoSys Ltd. regisztrált védjegye. A dokumentumban előforduló egyéb márka és termékeknek az azonosítást szolgálják és jogaikkal tulajdonosaik rendelkeznek.



Endpoint Protector 2009 Műszerfal  
Jelentéskészítő & Adminisztratív eszköz

- Endpoint Security
- Data Loss Prevention
- Portable Device Management
- Data Theft Prevention
- Data Monitoring
- Analysis & Reporting
- Data Transfer Monitoring
- File Tracing
- Data Encryption and Sync
- Protecting sensitive data in transit



Endpoint Protector 2009 három pillerre épül  
Megelőzés - Monitorizálás - Adatvédelmi kódolás