



## McAfee Device Control

### Meggátolja a csatlakoztatható eszközök jogtalan használatát

Habár az USB eszközök, mp3 lejátszók, CD-k, DVD-k gyakran használtak a vállalatokon belül, de mindegyik potenciális biztonsági kockázatot jelent. A kis méretükből, és nagy kapacitásukból fakadóan könnyedén másolhatók érzékeny adatok ezen tárolókra, mely rossz kezekben, vagy lopás esetén nagy kockázatot rejt. Egy felmérés során a vállalatok 55%-a elismerte, hogy a felhasználóik szabadon rendelkeznek a saját tárolóeszközeikkel, melyen akár érzékeny adatok is lehetnek. Ez több kérdést is felvet:

- hogyan ellenőrizhető, hogy mely felhasználónál vannak érzékeny adatok?
- hogyan ellenőrizhető, hogy milyen tároló eszközök vannak használatban?
- hogyan ellenőrizhető az adatok biztonságos tárolása?

#### Jellemzők

##### Teljes védelem

- Mindegy, hogy hol dolgozik, a munkahelyén, otthon, vagy akár utazik.

##### Egyedülálló eszköztámogatás

- Tartalom, hardver alapú szűrések, blokkolások hozhatók létre, a teljes forgalom ellenőrizhető bármilyen munkaállomáshoz csatlakoztatható tárolóeszközön

##### Egyedülálló jogosultság alapú hozzáférés

- Nincs szükség minden USB eszköz tiltására, különböző jellemzők alapján kontrollálhatók az eszközök

##### ePO alapú központi menedzsment

- A McAfee integrált menedzsment konzoljáról megoldható a termék teljes felügyelete

##### Teljes átláthatóság

- Az auditorok munkáját segíti a belső, iparági szabványok ellenőrzése, és automatikus riportkészítési modulja

#### Gátolja meg az adatvesztést

Az adatvesztés az egyik legveszélyesebb, „legdrágább” probléma (egy adatvesztés átlagos kárértéke 6,3 millió USD), melyre a cégeknek számítani kell. A Fortune1000 vállalatok 75%-a ismerte el már, hogy kerültek ki érzékeny adatok a hálózatáról.

#### Védje adatait a csatlakoztatható eszközökön is

A McAfee Device Control megelőzi az adatvesztést a csatlakoztatható tárolóeszközökön keresztül, mint például: USB stick, iPod, Bluetooth eszköz, CD, vagy DVD. Egy központi menedzsment megoldással szabályozható a hozzáférés, függetlenül a felhasználótól, a kliens típusától még a vállalati hálózaton kívül is.

A termék nagyon részletes szabályrendszerrel konfigurálható a felhasználói igényeknek megfelelően. Nemcsak tiltani, de engedélyezni is lehet eszközöket, felhasználókat, adattípusokat file szervereket, alkalmazásokat.

#### Készítsen részletes szabályokat a hardvereszközeire

A szabályok kiépítése egyszerű, a McAfee ePo szerverrel ez könnyedén állítható. Telepíthető távolról a McAfee Device Control agent, mely a szabályrendszer végrehajtását ellenőrzi.

A McAfee Device Control segít a továbbiakban, elkészíti a szükséges riportokat, tárolja az eseményeket, a szabálysértéseket, az adatmódosítási kísérleteket (másolás, mozgatás, kivágás, tömörítés, titkosítás).

#### Megfelelőség vizsgálat

A McAfee Device Control teljes felügyeletet biztosít a vállalati érzékeny adatok felett, hiszen minden adatmozgás szabályozható a külső tárolóeszközökre.

A McAfee ePo integrációnak köszönhetően az események szűrhetők akár eszköztípus, akár adattípus, akár idő alapján, sőt a felhasználói tevékenység le is tárolható a későbbi bizonyításhoz.

A széleskörű riportoknak, előrejelzéseknek köszönhető, hogy az auditorok, elemzők munkája részben kiváltható.

## RENDSZER- KÖVETELMÉNYEK

### ePO Server

Operációs rendszer:

- Microsoft Server 2003 SP1, 2003 R2

Hardver követelmény

- HDD: 250 MB
- RAM: 512 MB (1 GB RAM az ajánlott)
- CPU: Pentium II (450MHz minimum)

### Device Control Endpoint

Operációs rendszer:

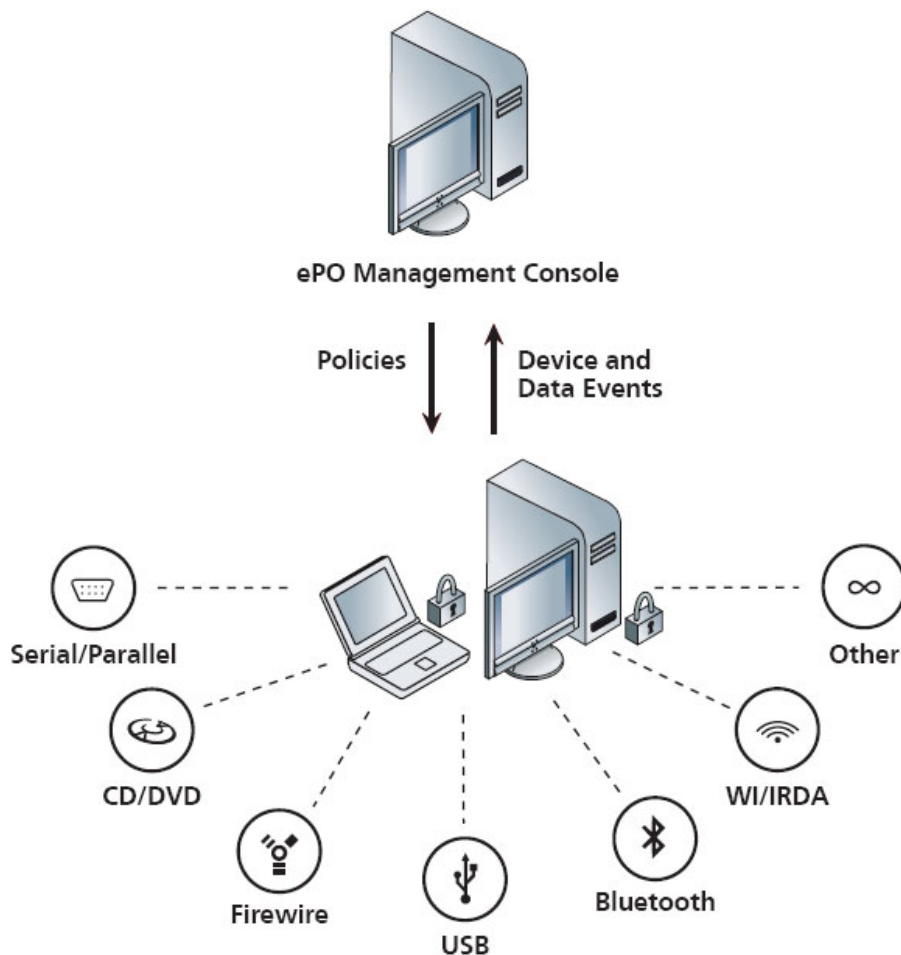
- Microsoft Windows XP Professional SP1, vagy újabb
- Microsoft Windows 2000 SP4, vagy újabb

Hardver követelmény:

- CPU: Pentium III (1 GHz minimum)
- RAM: 512 MB
- HDD: 200 MB
- Hálózat: TCP/IP

## Jellemzők

- Szabályozható a felhasználók hozzáférése (ki, milyen eszközre, mit másolhat)
- Számos eszköztípus támogatott (USB eszköz, iPod, CD, DVD, floppy, Bluetooth és infravörös)
- Ellenőrizhető a COM, LPT, soros, párhuzamos port is
- Az engedélyezett és tiltott csatlakoztatható eszközök kategóriákra bonthatóak, és külön szabályok is létrehozhatók. A szabályok alapja lehet bármilyen fizikai eszközparaméter, de akár a product ID, vendor ID, sorozatszám, device class is.
- Bármilyen adat ellenőrizhető akár mozgatás, másolás tömörítés, beillesztés, tömörítés után is
- A napi működésben semmilyen változást nem okoz
- Könnyen, központilag telepíthető, frissíthető, tilthatóak az eszközök
- A szabályrendszer lehet felhasználó, csoport, osztály alapú is
- Segíti az auditot a részletes log-bejegyzéseknek köszönhetően
- A szoftver fingerprint készítéssel (küldő, címzett, time stamp, file hash, evidence report) segíti a további elemzést. A megoldás több mint 390 fájl típust ismer, melyeket akár tag-el is képes ellátni (egy vízjelhez hasonló megoldás mely a fájlhoz van csatolva minden esetben).



A McAfee Device Control által felügyelt kommunikációs csatornák

További információkért keresse a McAfee Host DLP weboldalát:

[http://www.mcafee.com/uk/enterprise/products/data\\_protection/data\\_loss\\_prevention/device\\_control.html](http://www.mcafee.com/uk/enterprise/products/data_protection/data_loss_prevention/device_control.html)