

# GFI EndPointSecurity

Biztonsági megoldás a hordozható adattárolók ellenőrzésére

Az USB pendrive-ok, Bluetooth-képes okos telefonok, digitális kamerák és zenelejátszók akár több tíz gigabájtnyi adat tárolására képesek, és mindenfajta informatikai felügyelet nélkül, közvetlenül csatlakoztathatók a munkaállomásokhoz vagy notebookokhoz. A hordozható adattároló eszközök mindegyike lehetőséget teremthet az adatszivárgásra- vagy lopásra. Az adatszivárgás és az adatlopás megakadályozására fejlesztette ki a GFI az EndPointSecurity terméket.

## Az adatlopás és a fertőzések megakadályozása

A hordozható adattároló eszközökre egy cég vagy intézmény szinte összes bizalmas adata ráfér, vagy rajtuk keresztül akár vírusok, kémprogramok, jogsértő tartalmak is bejuttathatók a vállalati hálózatba. A GFI EndPointSecurity segítségével a hálózat üzemeltetői vagy biztonsági felelősei ezt a csatornát is képesek ellenőrizni és megakadályozni, hogy nem kívánt tartalmak jussanak be a hálózatba, vagy bizalmas adatok jussanak ki a hálózatból, továbbá fájl típusonként szabályozhatóak a hozzáférések (például: \*.doc olvasható, a \*.exe fájlhoz tiltott a hozzáférés).

## Port- és eszközmenedzsment egyszerűen

A csatlakozások megakadályozásához és felügyeletéhez a GFI EndPointSecurity egy kisméretű kliensprogramot telepít fel a számítógépekre. Az integrált technológia a GFI LANguard remote deployment megoldásán alapszik, mely segítségével néhány kattintással akár több száz munkaállomáson is telepíthető vagy eltávolítható a kliens. A telepítés után a kliensprogram lekérdezi az Active Directory-t, majd beállítja a megfelelő jogosultságokat. Ha a felhasználó nem tagja olyan csoportnak, amelynek engedélyezett a csatlakoztatás, a GFI EndPointSecurity blokkolja a csatlakozó eszközöket.

Blokkolható eszközök például: USB, FireWire, Bluetooth, Infrared, Wi-Fi, PCMCIA, Parallel, Serial, S-ATA, SD.

## Hordozható adattárolók ellenőrzése és kontrollja

Az USB csatlakozású adathordozók méretükből és tárolókapacitásukból adódóan az egyik legfőbb veszélyforrást képviselik, mert csaknem észrevehetetlenek és

akár sok száz Gb-nyi adat is elfér rajtuk. A legegyszerűbb példa, ha a felhasználó a digitális kameráját csatlakoztatja a munkahelyi számítógépe USB portjára. A GFI EndPointSecurity érzékeli a digitális kamera csatlakoztatását, és a jogosultságoknak megfelelően tiltja vagy engedélyezi az eszközt. Előfordulhat, hogy míg a digitális kamerák nemkívánatos eszköznek minősülnek, addig a szabványos USB kulcsok csatlakoztatását megengedi a vállalati szabályzat. A GFI EndPointSecurity ebben az esetben a kamera-eszközt nem engedi csatlakoztatni, de az USB kulcsot minden probléma nélkül használhatja a felhasználó.

## Adatmozgások naplózása

Az eszközökről vagy az eszközökre érkező adatokról, adatmozgásról minden esetben naplóbejegyzés keletkezik, így később visszaellenőrizhető, hogy ki milyen adatokat másolt. A GFI EndPointSecurity bevezetésével az üzemeltetők képesek ellenőrizni és naplózni a felhasználói aktivitást az alábbi eszközök esetén:

- Médialejátszók, iPod, Creative Zen, MS Zune, stb. készülékek
- USB eszközök, CompactFlash kártyák, memóriakártyák, nyomtatók, CD/DVD, floppy és más külső tároló eszközök
- PDA-k, BlackBerry készülékek, mobiltelefonok, okostelefonok vagy a kommunikációs portok
- Hálózati kártyák vagy más hálózati eszközök és csatlakozások használatakor

## Finomhangolható hozzáférés-ellenőrzés, fehér- és fekete listák

A GFI EndPointSecurity használatával engedélyezhetőek vagy tilthatóak eszközcsoportok, az adattranszfer (fájlok kiterjesztése alapján) a fizikai portokon vagy konkrét azonosítóval (factory ID) rendelkező eszközökön keresztül. Megadható, hogy bizonyos felhasználó



lók vagy csoportok teljes hozzáféréssel rendelkezzenek, és aktivitásuk csak naplózásra kerüljön. Összeállítható olyan eszköz fehér- vagy feketelista, amely csak a vállalat által elfogadott típusú eszközök csatlakoztatását engedi meg, és minden más eszközt letilt.

### Valós idejű monitorozás és riasztás

Valós idejű monitorozási lehetőségek érhetőek el a grafikus felhasználói felületen, az üzemeltetők pontos információkat kaphatnak a kliensek állapotáról, a felhasználók sikeres aktivitásáról (pl.: USB használat), vagy házirend alapján tiltás alá eső kísérletekről, vagy a kliensprogramok állapotáról. A GFI EndPointSecurity képes email, hálózati üzenet vagy SMS alapú riasztásokat és értesítéseket küldeni, például meghatározott eszközök csatlakozási kísérletekor.

### Felhasználóbarát felület

A kliensen futó GFI EndPointSecurity állapota és események statisztikája a felhasználó által is ellenőrizhető, ezzel segítve a biztonság tudatos használatot. Blokkolt eszközök esetében az üzemeltetők számára lehetőség van egyedi rendszerüzenetek küldésére.

### Minden eszközre és aktivitásra kiterjedő riportolási lehetőség

A GFI ReportPack kiegészítő komponens segítségével mindenre kiterjedő, IT- és menedzsment szintű, részletes riportok készíthetők akár ütemezetten és automatikusan. A GFI ReportPack csomag segítségével az üzemeltetők vagy a biztonsági felelősök pontos képet kaphatnak a csatlakozott eszközökről, az adattranszferokról, és mozgatott fájlokról is.

### További szolgáltatások

- Csatlakozó vagy már csatlakoztatott eszközök keresése és vizsgálata,

- A kliensprogram csak jelszó birtokában távolítható el,
  - Testre szabható és informatív felhasználói üzenetek blokkolásakor,
  - A felhasználói aktivitás monitorozása és az eszközhasználat ellenőrzése a központi adatbázis segítségével,
  - Automatikus vagy manuális adatbázis-funkciók, a régi vagy elévült adatok eltávolítására,
  - Unicode kódkészlet támogatása,
- Egyszerűen konfigurálható, csoportszintű, Active Directory alapú port- és eszközmenedzsment.

### Automatikus klienstelepítés

Ha az üzemeltető vagy a biztonsági felelős összeállította vagy módosította a szabályrendszert, a kliensek kitelepitését időzítheti és automatikusan elvégeztetheti. Ha a telepítés nem sikerül (a gép nem volt a hálózatra csatlakoztatva), a GFI EndPointSecurity újraütemezi, és addig próbálja a kliensalkalmazás kitelepitését, amíg nem sikerül. A telepítés Active Directory segítségével is megtörténhet: a GFI EndPointSecurity összeállítja az MSI telepítőkészletet, amely tartalmazza az egyéni biztonsági beállításokat, így akár a bejelentkezéskor is feltelepülhet.

### Ideiglenes és delegált eszközhozzáférés

Előfordulhat, hogy a felhasználó munkájához valóban szükséges a külső eszköz csatlakoztatása. Az üzemeltető ilyen esetekben ideiglenes és időszakos hozzáféréseket engedélyezhet az eszközhöz vagy eszközcsoporthoz, amely még akkor is működik, ha már a számítógép nincs a hálózathoz csatlakoztatva és a kliensalkalmazás nem tud kommunikálni a központtal. Bizonyos felhasználói kör (kiemelt felhasználók) részére folyamatos, teljes elérés biztosítható az amúgy védett eszközökhöz.

### Rendszerkövetelmények

- x86: Windows XP, Vista, 2000(SP4)/2003/2008
- x64: Windows XP, Vista, 2003/2008
- Internet Explorer 5.5 vagy magasabb
- .NET Framework 2.0, adatbázis szerver, SQL Server 2000, 2005, 2008
- 1116-os TCP port engedélyezése

### Díjak



### Az Ön viszonteladója:

