

▪ GfiEndpointSecurity



Biztonsági megoldás a hordozható adattárolók ellenőrzésére

Az USB pendrive-ok, Bluetooth-képes okostelefonok, 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. Ennek 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 onnan.

▪ Port- és eszközmenedzsment egyszerűen

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

▪ Hordozható adattárolók ellenőrzése és kontrollja

Az USB csatlakozású adathordozók méretükből és tárolókapacitásukból adódóan az egyik legfőbb veszélyforrást képviselik, mert csaknem észrevehetetlenek és akár 4Gb-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 nem kívánatos 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 ki az eszközre. A GFI EndPointSecurity bevezetésével az üzemeltetők képesek ellenőrizni és naplózni a felhasználói aktivitást az alábbi eszközök esetén:

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

- **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 felhasználók vagy csoportok teljes hozzáféréssel rendelkezzenek, és aktivitásuk csak naplózásra kerüljön. Összeállítható olyan fehér- és fekete eszközlista, amely csak a vállalat által elfogadott típusú eszközök csatlakoztatását engedi meg, és minden más letilt.

- **Valós idejű monitorozás és riasztás**

Valós idejű, monitorozási lehetőségek érhetőek el a grafikus felhasználói felületen, az üzemeltetők pontos információkat kaphatnak a felhasználók aktivitásáról vagy a kliensprogramok működéséről. A GFI EndPointSecurity képes e-mail, hálózati üzenet vagy SMS-alapú riasztásokat és értesítéseket küldeni, például meghatározott eszközök csatlakozási kísérletekor.

- **Minden eszközre és aktivitásra kiterjedő riportolási lehetőség**

A GFI ReportPack kiegészítő komponens segítségével mindenre kiterjedő, IT- és menedzsmentszint, 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 adattranszferekről és a mozgott 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, csoportszint, ActiveDirectory alapú port- és eszközmenedzsment.

- **Automatikus klienstelepítés**

Ha az üzemeltető vagy a biztonsági felelős összeállította vagy módosította a szabályrendszert, a kliensek kitépítését 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 kitépítését, amíg nem sikerül. A telepítés ActiveDirectory segítségével is megtörténhet, a GFI EndPointSecurity összeállítja az MSI telepítőkészletet, amely akár a bejelentkezéskor is feltelepülhet.

- **Ideiglenes 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.

- **Rendszerkövetelmények:**

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

