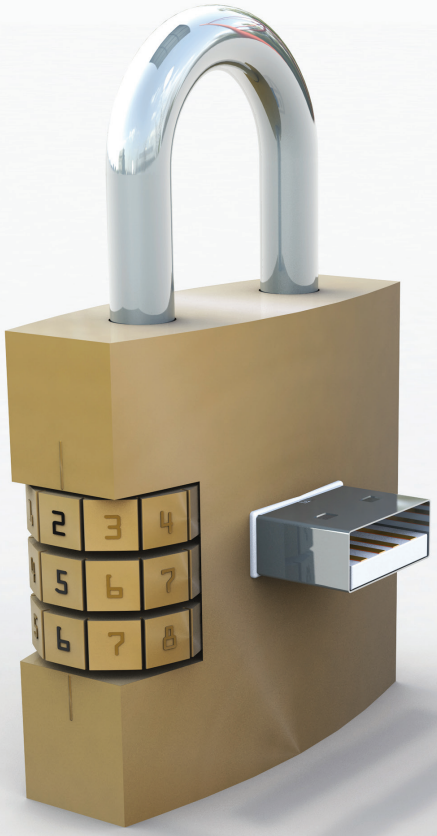
Uitgebreide controle op het gebruik van USB-opslagapparaten en andere draagbare media



- Gegevensherkenning
- Beoordeling van het risico op gegevenslekken
- Toegangscontrole

Window Security.com READERS' CHOICE WINNER

SC MAGAZINE

OPSWAT. BRONZE CERTIFIED Device Access Control

Ontdek meer en start uw GRATIS testversie:

gfi.com/endpointsecurity

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

GFI EndPointSecurity™

Controle over USB-sticks, iPod's en andere apparaten van eindgebruikers

Uitgebreide controle op het gebruik van USB-opslagapparaten en andere draagbare media

Het veelvuldige gebruik van consumentenapparaten zoals smartphones, mediaspelers, draagbare opslagapparaten, apparaten die op netwerken zijn aangesloten en gemakkelijk te verbergen USB-sticks, heeft het risico vergroot op gegevenslekken, virusinfecties, gebruik van software zonder licenties, games en andere kwaadaardige activiteiten in netwerken.

Terwijl de meeste ondernemingen gebruikmaken van antivirus, firewalls, contentbeveiliging voor e-mail en het web om hun netwerken te beschermen tegen externe bedreigingen, zijn er slechts enkele ondernemingen die beseffen hoe gemakkelijk werknemers een grote hoeveelheid vertrouwelijke en commercieel gevoelige informatie naar een draagbaar opslagapparaat kunnen kopiëren zonder dat iemand dat weet.

Fysiek alle USB-poorten blokkeren is moeilijk haalbaar en niet realistisch. Het geheim voor een succesvol beheer van het gebruik van draagbare media, is de installatie van een oplossing voor eindpuntbeveiliging waarmee beheerders kunnen beheren welke apparaten worden gebruikt, welke apparaten zijn gebruikt en door wie welke gegevens werden gekopieerd.

Hoe het werkt

GFI EndPointSecurity installeert automatisch een sabotagebestendige verborgen agent op de machines in uw netwerk om controle uit te oefenen op de toegang. Deze agent kan netwerkbreed met slechts een paar klikken op machines worden geïnstalleerd. Deze agent biedt een ongeëvenaarde sabotagebeveiliging, zelfs tegen gebruikers met beheerdersrechten. IT-beheerders houden met deze oplossing daarom altijd de controle over wat er gebeurt.

Controleer gebruikerstoegang en bescherm uw netwerk tegen bedreigingen van draagbare opslagmedia

Met GFI EndPointSecurity kunt u de toegang tot draagbare opslagmedia voor gebruikers centraal blokkeren. Op deze manier kunt u voorkomen dat gebruikers gegevens stelen of schadelijke gegevens het netwerk binnenbrengen. Hoewel u vanuit de BIOS een aantal fysieke poorten kunt uitschakelen, is deze oplossing in de praktijk niet efficiënt genoeg omdat geavanceerde gebruikers de BIOS met gemak kunnen hacken. Met GFI EndPointSecurity kunt u een groot aantal verschillende apparaten beheren.

Registreer de activiteiten van draagbare apparaten die toegang krijgen tot uw netwerk

Behalve dat met GFI EndPointSecurity toegang tot opslagmedia kan worden geblokkeerd, wordt door GFI EndPointSecurity ook de gebruikersactiviteit met betrekking tot apparaten geregistreerd, zowel in een event log als op een centrale SQL Server. Telkens wanneer iemand een geautoriseerd apparaat inplugt, wordt een overzicht geregistreerd van bestanden die op een bepaald apparaat zijn gebruikt.

Versleutel draagbare apparaten

Aan gebruikers kan toestemming worden gegeven om op USB-apparaten gegevens op te slaan zolang deze versleuteld zijn. Toegang tot deze gegevens buiten het bedrijfsnetwerk kan strikt worden geregeld door een specifiek ontwikkelde reisapplicatie, die inbegrepen is in GFI EndPointSecurity.

Andere kenmerken:

- Wizard voor het aanmaken van een beleid gericht op geavanceerde en gedetailleerde controle
- Dagelijkse/wekelijkse overzichten
- Real-time statusbewaking en real-time meldingen
- Volledige rapporten over het gebruik van apparaten met de GFI ReportPack-add-on
- Ondersteunt Windows 7 BitLocker To Go
- Verzendt aangepaste pop-ups naar gebruikers wanneer zij geen toestemming hebben om een apparaat te gebruiken
- Maakt het via een backend-database mogelijk te bladeren door logs met informatie over gebruikersactiviteiten en mediagebruik
- Kan computers groeperen per afdeling, domein, enz.
- Ondersteunt besturingssystemen in alle Unicode-talen
- En meer!

Start uw gratis testversie op **gfi.com/endpointsecurity**

Voordelen in één oogopslag

- Voorkomt lekkage of diefstal van gegevens door de toegang tot draagbare opslagmedia met minimaal beheer te controleren
- Voorkomt door middel van encryptie dat gegevens per abuis worden gelekt wanneer verwisselbare opslagapparaten worden gestolen of verloren raken
- Beoordeelt het risico op gegevenslekkage die wordt veroorzaakt door verwisselbare apparaten op eindpuntniveau en geeft informatie over hoe dit risico kan worden verlaagd
- Beschermt gegevens onderweg met behulp van encryptie van verwisselbare volumes
- Stelt beheerders in staat om apparaten te blokkeren op basis van klasse, bestandsextensies, fysieke poort of apparaat-id
- Stelt beheerders in staat het gebruik van media of poorten voor een beperkte periode toe te staan

Ga voor een compleet overzicht met voordelen naar:
www.gfi.com/endpointsecurity

Systeemvereisten

Windows 2000 (SP4), XP, Vista, 7 en 8, Windows Servers 8 en 2012 (x86- en x64-versies)

Internet Explorer 5.5 of hoger

.NET Framework versie 4.0

Poort: TCP poort 1116 (standaard)

Database-backend: SQL Server 2000/2005/2008; als deze niet beschikbaar is, kan GFI EndPointSecurity automatisch een versie van SQL Server Express downloaden, installeren en configureren.

GFI®
www.gfi.nl

Ga voor een volledig wereldwijd overzicht van kantoren en contactgegevens van GFI naar:
www.gfi.com/contact-us