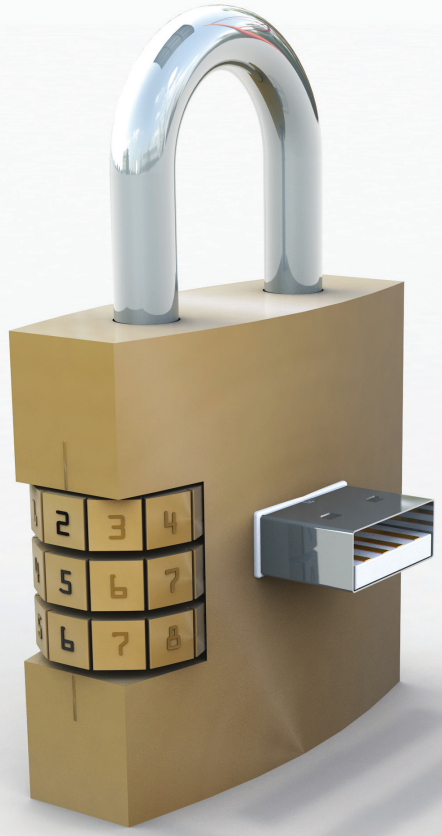
Controllo completo dell'utilizzo di memorie USB e altri dispositivi portatili



- Conoscenza dei dati
- Valutazione del rischio di fuga dei dati
- Controllo di accesso

Window Security.com READERS' CHOICE WINNER

SC MAGAZINE

OPSWAT. BRONZE CERTIFIED Device Access Control

Scopritene di più e cominciate la vostra prova GRATUITA:

gfi-italia.com/endpointsecurity

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

GFI EndPointSecurity™

Controllo di chiavi USB, iPod e altri dispositivi endpoint

Controllo completo dell'utilizzo di memorie USB e altri dispositivi portatili

Il proliferare di dispositivi di consumo quali smartphone, riproduttori multimediali, dispositivi di memoria portatili, dispositivi connessi alla rete e chiavi USB facilmente occultabili ha aumentato il rischio di fuga di dati, infezioni da virus, introduzione di software e giochi senza licenza e altre attività pericolose sulle reti.

Sebbene gran parte delle aziende disponga di antivirus, firewall e protezione della posta elettronica e del contenuto web per tutelarsi dalle minacce esterne, poche si rendono conto della facilità con cui un dipendente può copiare enormi quantità di dati riservati o sensibili dal punto di vista commerciale su un dispositivo di memoria portatile all'insaputa di tutti.

Bloccare fisicamente tutte le porte USB non è né sostenibile né fattibile. La chiave per gestire l'utilizzo di dispositivi portatili consiste nell'installare una soluzione di sicurezza degli endpoint che offra agli amministratori il controllo sui dispositivi in uso, su quelli utilizzati e dei rispettivi utenti e fornisca loro una conoscenza approfondita dei dati eventualmente copiati.

Come funziona

Per controllare l'accesso, GFI EndPointSecurity installa automaticamente un agente nascosto e a prova di manomissione sui computer della rete. L'agente può essere distribuito sui computer di tutta la rete in soli pochi clic e fornisce una protezione senza pari dalle manomissioni, persino dagli utenti con diritti amministrativi, permettendo agli amministratori IT di rimanere sempre in controllo.

Gestione dell'accesso degli utenti e protezione della rete dalle minacce costituite dai supporti multimediali portatili

Utilizzando GFI EndPointSecurity potete disabilitare a livello centrale gli utenti dall'accesso a supporti di memoria portatili, impedendo così loro di rubare dati o immettere dati potenzialmente dannosi per la vostra rete. Sebbene possiate spegnere alcune porte di connessione fisiche dal BIOS, questa soluzione in realtà non è pratica e utenti esperti sono in grado di modificare il BIOS con facilità. GFI EndPointSecurity vi permette di assumere il controllo su un'ampia gamma di dispositivi.

Registrazione dell'attività dell'accesso di dispositivi portatili alla rete

Oltre a bloccare l'accesso a supporti di memoria portatili, GFI EndPointSecurity registra l'attività utente relativa a dispositivi sia nel registro degli eventi che in un Server SQL centrale. Ogni volta che si collega un dato dispositivo autorizzato, viene registrato un elenco dei file cui è stato effettuato l'accesso.

Crittografia di dispositivi portatili

Gli utenti possono essere autorizzati a memorizzare dati su dispositivi USB a condizione che siano crittografati. L'accesso a tali dati al di fuori della rete aziendale può essere rigorosamente controllato da un'apposita applicazione richiedente, compresa in GFI EndPointSecurity.

Altre funzionalità

- Creazione guidata di criteri/politiche ai fini di un controllo di accesso granulare avanzato
- Riepiloghi giornalieri o settimanali
- Monitoraggio dello stato e avvisi in tempo reale
- Rapporti completi sull'utilizzo dei dispositivi grazie al componente aggiuntivo GFI ReportPack
- Supporto di Bitlocker To Go di Windows 7
- Esplorazione dei registri dell'attività utente e di utilizzo dei dispositivi tramite un database terminale
- Possibilità di raggruppare i computer secondo il reparto, dominio, ecc.
- Supporto di sistemi operativi aderenti a qualsiasi linguaggio Unicode
- E molto di più!

Cominciate la vostra prova gratuita scaricandola da **gfi-italia.com/endpointsecurity**

Vantaggi in sintesi

Prevenzione fuga e furto di dati mediante il controllo dell'accesso a dispositivi di memoria portatili, con pochissima amministrazione

Prevenzione della perdita accidentale di dati in caso di perdita o furto dei dispositivi di memoria rimovibili, grazie all'utilizzo della crittografia

Valutazione del rischio di fuga di dati comportato dai dispositivi rimovibili a livello di endpoint e riporto di informazioni sulle modalità per attenuare tale rischio

Protezione dei dati durante i viaggi grazie alla crittografia a livello di volume del dispositivo rimovibile

Possibilità per gli amministratori di bloccare dispositivi secondo la classe, le estensioni dei file, la porta fisica o l'ID del dispositivo

Per leggere l'elenco completo dei vantaggi, visitate il sito:
www.gfi-italia.com/endpointsecurity

Requisiti di sistema

Windows 2000 (SP4), XP, Vista, 7 e 8, Windows Servers 8 e 2012 (versioni a 86 e 64 bit)

Internet Explorer 5.5 o successivi

.NET Framework versione 4.0

Porta: porta TCP 1116 (predefinita)

Terminale database: SQL Server 2000/2005/2008; qualora questi non fossero disponibili,

GFI EndPointSecurity può scaricare, installare e configurare automaticamente una versione di SQL Server Express.

GFI®
www.gfi-italia.com

Per leggere l'elenco completo degli uffici/recapiti GFI in tutto il mondo, visitate la pagina:
www.gfi-italia.com/contact-us

© 2015 GFI Software – Windows XP (SP 2), Vista, 7 e 8 sono marchi commerciali di Microsoft Corporation.

GFI EndPointSecurity è un marchio commerciale registrato e GFI e il logo GFI sono marchi commerciali di GFI Software in Germania, negli Stati Uniti, nel Regno Unito e in altri paesi.

Tutti i prodotti e le aziende citati nel presente documento possono essere marchi commerciali dei rispettivi proprietari.