USB-Sticks, MP3-Player und Smartphones öffnen Tür und Tor für Datendiebstahl und Viren – jetzt gegensteuern!

Leistungsstark und **intuitiv**

Überzeugende Funktionsvielfalt

Umfassende Kontrolle

Attraktives Preis-Leistungsverhältnis

Auch erhältlich als **FREEWARE**

Steuerung des Einsatzes von iPod®s, USB-Sticks und anderen mobilen Speichermedien im Netzwerk

Die breite Nutzung von iPods, USB-Sticks, Smartphones und anderen mobilen Massenspeichern in Unternehmen fördert nicht nur den Diebstahl und Verlust wichtiger Daten. Auch die Netzwerksicherheit ist bedroht. Zum Schutz vor Angriffen von außen sind in den meisten Fällen Antiviren-Software, Firewalls und sonstige Sicherheitslösungen für E-Mail und Internet-Nutzung im Einsatz. Doch Gefahren lauern auch firmenintern: Vielfach wird übersehen, wie einfach Mitarbeiter iPods oder USB-Sticks an Netzwerkrechner anschließen können. Vertrauliche und unternehmenskritische Daten sind binnen Minuten in großem Umfang kopiert – unbemerkt. Zudem können auf diesem Weg Viren und illegale Software ins System gelangen. Eine differenzierte Zugriffssteuerung ist daher unerlässlich. Das komplette Sperren aller USB-Schnittstellen ist jedoch keine praktikable Lösung, um Sicherheitsrisiken zu minimieren – die Alternative lautet GFI EndPointSecurity™.

VORTEILE

- Verwaltungsfreundliche Zugriffssteuerung für tragbare Speichermedien zur Verhinderung von Datenabfluss und -diebstahl
- Datensicherheit bei Diebstahl oder Verlust von Wechselspeichern dank Verschlüsselung
- Bewertung des Datenleck-Risikos durch tragbare Speichermedien für alle Endgeräte plus empfohlene Schutzmaßnahmen
- Regulierung der Datenübertragung unter Berücksichtigung von Dateiinhalt und tatsächlichem Dateityp
- Unterbindung der Übertragung von Malware und unerwünschter Software ins Netzwerk
- Gerätesperrung nach Kategorie, Dateierweiterung, Schnittstelle oder sogar Seriennummer
- Zeitlich begrenzbare Freigabe von Geräten oder Schnittstellen
- Optionales, automatisches Herunterladen und Installieren von Microsoft SQL Server Express bei nicht vorhandenem Datenbank-Server

GFI EndPointSecurity™

Kontrolle von iPods, USB-Sticks und anderen mobilen Endgeräten

Verhinderung von Datendiebstahl und Malware-Infektionen durch interne Quellen

Unternehmen, die sich der Gefahren durch tragbare Speichermedien bewusst sind und sie richtig einschätzen, können Schäden leichter vermeiden. Doch nur wenige KMU sehen tragbare Massenspeicher als größere Bedrohung für ihr Netzwerk an: Unter 20 Prozent setzen Sicherheitslösungen zur Kontrolle dieser Geräte ein (Quelle: eMedia-Studie für GFI, USA). Zum Schutz vor internem Datenabfluss muss die Verwendung mobiler Speichermedien gezielt gesteuert werden. Auch sind genaue Angaben zu übertragenen Daten und Benutzern erforderlich. Ebenso wichtig ist es, Daten, die das Unternehmen z. B. per USB-Stick verlassen sollen, auf vertrauliche Inhalte zu überprüfen und verschlüsseln zu können.

Umfassende Kontrolle über tragbare Geräte im Netzwerk

Dank GFI EndPointSecurity™ können Administratoren aktiv verwalten, welche Anwender Zugriff auf mobile Speichermedien erhalten, und die Aktivitäten folgender Hardware protokollieren:

- Multimedia-/MP3-Player (iPods, Creative Zens und andere mobile Unterhaltungsgeräte)
- USB-Sticks, CompactFlash- und andere Speicherkarten, CDs, Disketten sowie weitere tragbare Speichermedien
- Smartphones wie iPhone und BlackBerry, Mobiltelefone und ähnliche Kommunikationsgeräte
- Schnittstellen, Laptops und andere mit dem Netzwerk verbundene mobile Endgeräte

Funktionsweise

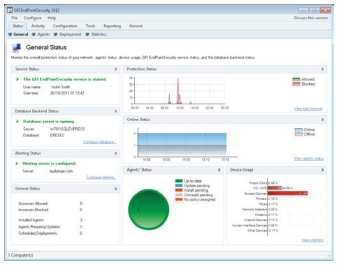
Zur Zugangskontrolle wird ein kompakter, für Anwender unsichtbarer Agent auf Benutzerrechnern im gesamten Netzwerk installiert – schnell und einfach.

Verwaltung des Benutzerzugriffs auf portable Speichermedien

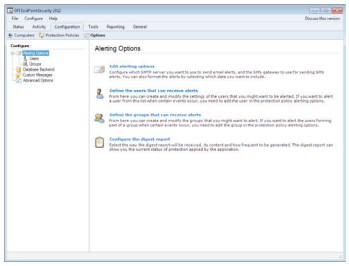
Legen Sie zentral fest, ob Benutzern ein Zugriff auf portable Speichermedien möglich sein soll. So verhindern Sie, dass Informationen über tragbare Geräte entwendet werden oder potenziell schädliche Daten wie Viren, Trojaner und andere Malware ins Netzwerk gelangen. Obwohl beispielsweise der CD- und/oder Diskettenzugriff über das BIOS deaktiviert werden kann, ist diese Lösung nicht sehr effizient: Zum Installieren neuer Software müsste der Zugriff direkt am Arbeitsplatz wieder manuell aktiviert werden. Zudem können erfahrene Anwender das BIOS problemlos manipulieren. GFI EndPointSecurity erlaubt eine gezielte Steuerung des Zugriffs auf zahlreiche Speichergeräte.

Zugriffsprotokollierung für portable Geräte im Netzwerk

Lassen Sie gerätespezifische Benutzerzugriffe im Ereignisprotokoll und in einer zentralen SQL-Server-Datenbank protokollieren. Auch auf portablen Speichermedien geöffnete Dateien werden stets genau erfasst.



Verwaltungskonsole



Konfigurationsoptionen

Verschlüsselung tragbarer Speichermedien

Legen Sie fest, dass Daten nur verschlüsselt auf USB-Medien gespeichert werden dürfen. Ein spezielles Traveler-Tool gestattet es berechtigten Anwendern, auch außerhalb des Netzwerks auf entsprechend geschützte Dateien zuzugreifen.

Inhaltsprüfung für übertragene Dateien

GFI EndPointSecurity erkennt den tatsächlichen Dateityp übertragener Dateien und überprüft ihren Inhalt zusätzlich anhand von vorgegebenen und selbst definierbaren regulären Ausdrücken und Wortlisten. Spüren Sie sicherheitsrelevante Informationen wie Kreditkartennummern, PINs u. v. m. in Dateien gängiger Formate auf, um die Übertragung zu blockieren.

Weitere Funktionen

- Zentrale Überwachung des Netzwerks auf mobile Speichermedien – Identifizierung verbundener Geräte und Durchführung von Aufgaben zur Zugriffssicherung
- Richtlinien-Assistent
- Täglicher/wöchentlicher Überwachungsbericht
- Automatischer Zugriffsschutz für neu erkannte Computer
- Optionales automatisches Herunterladen und Installieren von Microsoft SQL Server Express als Datenbank
- Granulare Zugriffssteuerung und Einrichtung von Whitelists/Blacklists
- Statusüberwachung und Warnungen in Echtzeit
- Umfassende Berichte zur Verwendung mobiler Speichermedien mit dem Zusatzmodul GFI ReportPack
- Einfache Hintergrund-Installation des Agenten zur Zugriffssteuerung
- Erteilung zeitlich begrenzter Gerätezugriffe
- Suche und Identifizierung von aktuell und zuvor verwendeten Geräten
- Passwortschutz für Agenten zur Zugriffskontrolle (auch unter Microsoft Windows 7)
- Unterstützung von Microsoft Windows 7 BitLocker To Go
- Individuell anpassbare Popup-Meldungen zu Gerätesperrungen für Benutzer
- Backend-Datenbank zur Sicherung und Anzeige von Benutzeraktivitäten und Geräteverwendung
- Wartungsfunktion zum Löschen älterer protokollierter Daten
- Einrichtung von Computer-Gruppen für Abteilungen, Domänen u. Ä.
- Unterstützung Unicode-kompatibler Betriebssysteme
- u. v. m.

Systemanforderungen

- Betriebssystem: Microsoft Windows 2000 (SP4), XP, 2003, Vista, 7 und 8 sowie Windows Server 2008 und 2012 (32- und 64-Bit-Versionen)
- Microsoft Internet Explorer 5.5 oder höher
- Microsoft .NET Framework 4.0
- Port: TCP-Port 1116 (Standard)
- Datenbank-Backend: Microsoft SQL Server 2000/2005/2008; falls nicht verfügbar, kann mit GFI EndPointSecurity Microsoft SQL Server Express automatisch heruntergeladen, installiert und konfiguriert werden.

Kostenfreie Testversion: http://www.gfisoftware.de/endpointsecurity

Microsoft Partner
Gold Independent Software Vendor (ISV)

GFI EndPointSecurity™

Kontrolle von iPods, USB-Sticks und anderen mobilen Endgeräten

Kontaktinformationen

Malta	GB	USA	Deutschland
Tel.: +356 2205 2000	Tel.: + 44 (0)870 770 5370	Tel.: +1 (888) 243-4329	Tel.: +49 (0) 69 22 22 73 12
Fax: +356 2138 2419	Fax: + 44 (0)870 770 5377	Fax: +1 (919) 379-3402	Fax: +49 (0) 69 2 22 22 64 78
sales@gfi.com	sales@gfi.co.uk	ussales@gfi.com	sales@gfisoftware.de

Weitere Niederlassungen von GFI finden Sie hier: http://www.gfisoftware.de/company/contact.html

GFI
www.gfisoftware.de