

Verfügbar in folgenden
Sprachen



Microsoft
GOLD CERTIFIED
Partner

GFI EndPointSecurity™

Steuerung des Einsatzes von iPods, USB-Sticks und anderen tragbaren Geräten im Netzwerk



- Leistungsstark und intuitiv
- Überzeugende Funktionsvielfalt
- Umfassende Kontrolle
- Starkes Preis-Leistungsverhältnis

Schutz des Netzwerks vor tragbaren Geräten wie USB-Laufwerken, iPods und PDAs

Laut Untersuchungen der Marktforscher des Ponemon Institute entwendeten 59 % der entlassenen Mitarbeiter vertrauliche Firmendaten auf DVD oder USB-Stick. Die weite Verbreitung von Smartphones, USB-Laufwerken, iPods und anderen mobilen Unterhaltungsgeräten erhöht zunehmend das Risiko von Datendiebstahl und -verlust und bedroht die Netzwerksicherheit. Zum Schutz vor Angriffen von außen verwenden die meisten Unternehmen bereits Antiviren-Software, Firewalls und Sicherheitslösungen für E-Mail- und Web-Inhalte. Doch Gefahren lauern auch firmenintern: Vielfach wird übersehen, wie einfach Mitarbeiter iPods oder USB-Sticks an Netzwerkrechner anschließen können. Vertrauliche Daten sind binnen Minuten in großem Umfang kopiert. Zudem können auf diesem Weg Viren und illegale Software ins System gelangen – eine differenzierte Zugriffssteuerung ist daher unerlässlich. Das komplette Sperren aller Schnittstellen ist hingegen keine praktikable und dauerhafte Lösung, um Sicherheitsrisiken zu minimieren.

Zahlreiche Unternehmen sind sich nicht bewusst oder blicken einfach darüber hinweg, welche großen Gefahren vom Einsatz tragbarer Speichermedien im Firmennetzwerk ausgehen – bis der Ernstfall eintritt und Daten durch Missgeschick oder Böswilligkeit abhanden kommen. Vor allem angesichts der aktuellen wirtschaftlichen Lage sind Cybercrime und Datenabfluss auf dem Vormarsch. Endpunkte am Arbeitsplatz sind ein beliebtes Ziel für Informationsdiebstahl. Schützen Sie sich vor dieser Bedrohung: mit GFI EndPointSecurity. Risiken durch portable Medien lassen sich jedoch nur mindern, indem Administratoren unmittelbar steuern können, welche Geräte im Firmennetzwerk eingesetzt werden dürfen. GFI EndPointSecurity™ bietet diese Möglichkeit und erlaubt es Systemverantwortlichen sogar, den Einsatz tragbarer Massenspeicher durch einzelne Mitarbeiter zu überprüfen – inklusive genauer Angaben zu ausgetauschten Daten.

VORTEILE

- **Unterbindung des Datenabflusses und -diebstahls durch eine verwaltungsfreundliche, umfassende Zugriffssteuerung für portable Speichermedien**
- **Erschwerung des Einschleppens von Malware und des Überspielens unerwünschter Software ins Netzwerk**
- **Differenzierte Zugriffskontrolle, auch unter Berücksichtigung von Dateierweiterungen – Gerätesperrung nach Kategorie, Schnittstelle oder sogar Seriennummer**
- **Zeitlich begrenzte Freigabe von Geräten oder Schnittstellen**
- **Unterstützung von 32-Bit- und 64-Bit-Plattformen, u. a. Microsoft Windows 7, Windows Vista und Windows Server 2008**
- **“Certified for Windows Server® 2008” und Unterstützung von Microsoft Windows Vista**



Protokollierung der Aktivität portabler Geräte im Netzwerk

USB-Sticks sind eine der Hauptbedrohungen für Unternehmensumgebungen. Sie können sehr unauffällig transportiert werden und besitzen eine Kapazität von bis zu 128 GB. Selbst in Digitalkameras enthaltene SD-Karten lassen sich beim Verbinden der Kamera mit einem vernetzten Computer zur Datenspeicherung nutzen und bieten bis zu 32 GB Speicherplatz. Daten können somit auf unterschiedlichste Weise entwendet oder auch eingeschleust werden. GFI EndPointSecurity erlaubt neben der Zugriffssteuerung zudem ein Protokollieren gerätespezifischer Benutzerzugriffe im Ereignisprotokoll und in einer zentralen SQL-Server-Datenbank. Auch auf portablen Speichermedien geöffnete Dateien werden genau erfasst.

Steuerung des Benutzerzugriffs auf tragbare Geräte im Netzwerk

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 sich beispielsweise CD- und Diskettenlaufwerke über das BIOS eines Computers deaktivieren lassen, ist diese Lösung nicht sehr effizient, insbesondere bei Software-Aktualisierungen. Zum Installieren neuer Programme oder Geräte müsste der Zugriff vom Administrator vor Ort manuell reaktiviert und danach wieder gesperrt werden. Zudem können erfahrene Anwender das BIOS problemlos manipulieren und Sicherheitsmaßnahmen umgehen. GFI EndPointSecurity erlaubt eine gezielte Steuerung des Zugriffs auf zahlreiche Geräte:

- Diskettenlaufwerke
- CD- und DVD-ROM-Laufwerke
- MP3-/Media-Player (z. B. iPod)
- tragbare Massenspeicher
- Drucker
- PDAs
- Netzwerkkarten
- Modems
- Bildverarbeitungsgeräte
- u. v. m.

Unterstützung von Microsoft Windows 7 und BitLocker To Go

Mit Microsoft Windows 7 steht die neue Funktionalität "BitLocker To Go" zur Verfügung, die Daten auf portablen Speichergeräten verschlüsselt. GFI EndPointSecurity 4.2 erkennt entsprechend geschützte Hardware und ermöglicht es, ihr unterschiedliche Zugriffsrechte zuzuweisen.

Funktionsweise

Zur Zugangskontrolle wird ein kompakter Agent auf dem Benutzerrechner installiert. Der Agent ist nur 1,2 MB groß und bleibt vom Anwender unbemerkt. Mit Hilfe eines Tools zur Remote-Installation, das auf der Technologie von GFI LANguard™ basiert, stellt GFI EndPointSecurity den Agenten mit nur wenigen Mausklicks auf Hunderten von Rechnern bereit. Nach der Installation startet das Überwachungs-Tool beim Anwender-Login eine Active-Directory-Abfrage. Berechtigungen für portable Geräte werden wie gewünscht festgelegt. Anwender erhalten danach nur Zugriff auf ein Gerät, für das sie als Mitglied einer Gruppe eingetragen sind.

Einfache Konfigurierung von Schutzgruppen per Active Directory

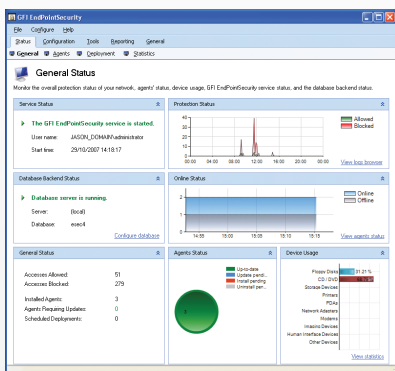
Ordnen Sie Computer in Schutzgruppen ein, denen unterschiedliche tragbare Geräte mit verschiedenen Zugriffsrechten zugewiesen werden. Beispielsweise lassen sich alle PCs einer Unternehmensabteilung gruppieren, um deren Einstellungen übergreifend, einheitlich und zeitsparend zu verwalten. GFI EndPointSecurity nutzt außerdem die Vorteile von Active Directory und bietet somit eine schnelle Konfigurierung und Verwaltung. Administratoren müssen Zuweisung und Art der Richtlinien für jeden einzelnen Benutzer-PCs nicht länger ständig parat haben. Hingegen ist bei anderen Überwachungslösungen jeder einzelne Netzwerkcomputer vor der Überwachung aufwendig zu konfigurieren und später auch getrennt zu aktualisieren.

Weitere Funktionen

- Erlaubt die Suche und Identifizierung von vor Kurzem oder aktuell verwendeten Geräten
- Bietet individuell anpassbare Popup-Meldungen für Gerätesperrungen
- Liefert Wartungsfunktion zum Löschen älterer Protokolldaten
- Läuft unter allen Unicode-kompatiblen Betriebssystemen

Systemanforderungen

- Microsoft Windows Server 2008/2003, Windows 2000 (SP4) oder Windows 7/Vista/XP (x86 und x64)
- Microsoft Internet Explorer 5.5 oder höher
- Microsoft .NET Framework 2.0
- Datenbank-Backend: Microsoft SQL Server 2008/2005/2000
- Port: TCP-Port 1116 (Standard)



Verwaltungskontrolle

Weitere Informationen und eine kostenfreie Testversion stehen zum Abruf bereit auf <http://www.gfi.com/de/endpointsecurity/>

Microsoft
GOLD CERTIFIED
Partner

Kontaktinformationen

Malta
Tel +356 2205 2000
Fax +356 2138 2419
sales@gfi.com

UK
Tel +44 (0)870 770 5370
Fax +44 (0)870 770 5377
sales@gfi.co.uk

USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
ussales@gfi.com

Asien/Pazifikraum/Südastralien
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI

www.gfi.com