



# GFI EndPointSecurity

Umfassende Steuerung des Einsatzes von iPods, USB-Laufwerken und anderen tragbaren Geräten

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

- MP3-Player wie iPods, Creative Zens u. Ä.
- USB-Laufwerke, CompactFlash- und andere Speicherkarten, CDs, Disketten und weitere Wechselspeicher
- PDAs, BlackBerry-Geräte, Mobiltelefone, Smartphones und ähnliche Kommunikationsmedien
- Netzwerkkarten, angeschlossene Laptops und andere Netzwerkverbindungen

## ■ Funktionsweise

Zur Zugangskontrolle wird von GFI EndPointSecurity ein kompakter Agent mit geringen Ressourcenanforderungen auf dem Benutzerrechner installiert. Dieser Agent ist nur 1,2 MB groß und bleibt vom Anwender unbemerkt. Mit Hilfe seines Tools zur Remote-Installation, das auf der Technologie von GFI LANguard basiert, kann GFI EndPointSecurity den Agenten mit nur wenigen Mausklicks auf Hunderten von Rechnern bereitstellen. Nach der Installation startet das Überwachungs-Tool beim Anwender-Login eine Active-Directory-Abfrage und legt die Berechtigungen für tragbare Geräte wie gewünscht fest. Anwender erhalten danach nur Zugriff auf ein Gerät, für das sie als Gruppenmitglied mit der jeweiligen Berechtigung eingetragen sind.

## Vorteile

### Warum GFI EndPointSecurity zur Zugriffskontrolle für tragbare Geräte?

- Verhindert Datenabfluss/-diebstahl durch eine verwaltungsfreundliche, umfassende Zugriffssteuerung für tragbare Speichermedien
- Erschwert das Einschleppen von Malware und das Überspielen unerwünschter Software ins Netzwerk
- Bietet Administratoren eine differenzierte Zugriffssteuerung, auch für Dateierweiterungen; Geräte lassen sich nach Kategorie, Schnittstelle oder sogar Seriennummer sperren
- Ermöglicht Systemverantwortlichen die zeitlich begrenzte Zugriffsfreigabe für Geräte oder Schnittstellen
- Unterstützt 32- und 64-Bit-Plattformen wie Microsoft Windows Vista und den aktuellen Release Candidate von Microsoft Windows Server 2008

## ■ Steuerung des Benutzerzugriffs zum Schutz des Netzwerks vor den Gefahren portabler Speichermedien

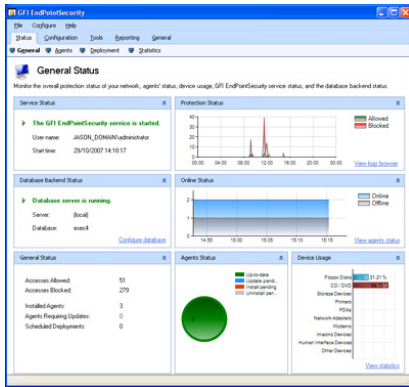
Mit GFI EndPointSecurity können Sie zentral festlegen, ob Benutzern ein Zugriff auf portable Speichermedien möglich sein soll. So verhindern Sie, dass Informationen über tragbare Geräte entwendet oder potenziell schädliche Daten wie Viren, Trojaner und andere Malware ins Netzwerk gelangen. Obwohl beispielsweise der CD- und/oder Diskettenzugriff über das BIOS deaktiviert werden kann, ist diese Lösung nicht sehr effizient: Zum Installieren neuer Software auf dem Rechner 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 Endgeräte wie:

- Diskettenlaufwerke
- CD- und DVD ROM-Laufwerke
- MP3-Player (iPod)
- tragbare Massenspeicher
- Drucker
- PDAs
- Netzwerkadapter
- Modems
- Bildverarbeitungsgeräte
- u. v. m.

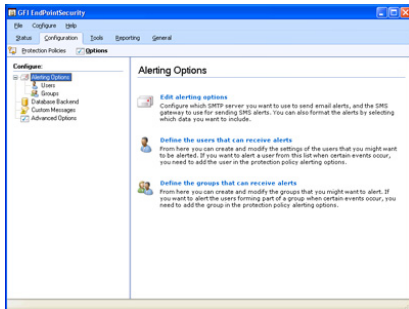
## ■ Protokollierung des Datenaustauschs über mobile Speichermedien wie USB-Sticks oder SD-Karten

USB-Sticks sind eine der Hauptbedrohungen für die Datensicherheit, weil sie sehr unauffällig transportiert werden können und eine Speicherkapazität von bis zu 4 GB besitzen. Verborgener Speicher steht auch zur Verfügung, wenn mit einem Netzwerkrechner eine Digitalkamera verbunden wird, von deren SD-Karte weitaus mehr digitale Daten abgerufen werden können als nur Fotos. GFI EndPointSecurity protokolliert gerätespezifische Benutzerzugriffe im Ereignisprotokoll und in einer zentralen SQL-Server-Datenbank. Auf portablen Speichermedien geöffnete und an/von Geräte(n) übertragene Dateien werden genau erfasst.

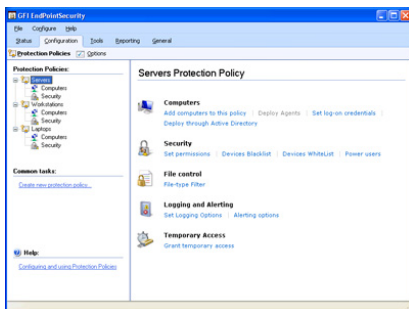
## GFI EndPointSecurity



Verwaltungskonsolle

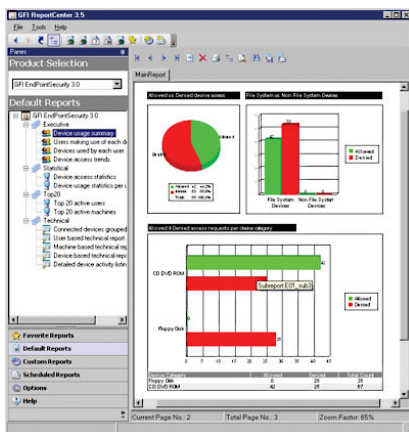


Konfigurationsoptionen



Standardmäßige Schutzrichtlinien

## GFI EndPointSecurity ReportPack



Bericht zur Geräteverwendung

## ■ Einfache Konfigurierung von Schutzgruppen per Active Directory

Ordnen Sie Computer in unterschiedliche Schutzgruppen ein, denen verschiedene Zugriffsrechte und tragbare Geräte, auf die (nicht) zugegriffen werden darf, zugewiesen werden können. Selbst eine gesamte Unternehmensabteilung kann als Mitglied einer Gruppe definiert werden, für die sich Einstellungen übergreifend ändern lassen. GFI EndPointSecurity nutzt die Vorteile von Active Directory und bietet somit eine schnelle Konfigurierung und Verwaltung – Administratoren müssen sich nicht länger um das Richtlinien-Management jedes einzelnen Rechners kümmern. Bei anderen Lösungen zur Speichermedien-Überwachung ist jeder Netzwerkrechner einzeln zu administrieren: Einstellungen sind vor der Überwachung mit hohem Aufwand getrennt zu konfigurieren und zu aktualisieren.

## ■ Granulare Zugriffssteuerung und Einrichtung einer Whitelist/Blacklist

Gestatten oder sperren Sie den Zugriff auf unterschiedliche Gerätekategorien, Schnittstellen oder sogar Seriennummern von Einzelgeräten. Zudem können Inhalte unter Berücksichtigung der Dateierweiterung blockiert werden. Durch die Einrichtung von Hauptbenutzern wird sichergestellt, dass befugte Benutzer oder Gruppen stets Vollzugriff auf tragbare Geräte erhalten. Administratoren haben auch die Möglichkeit, Devices, die stets oder nie zugänglich sein dürfen, auf eine Whitelist beziehungsweise Blacklist zu setzen.

## ■ Statusüberwachung und Warnungen in Echtzeit

Über die Verwaltungskonsolle von GFI EndPointSecurity ist eine Statusüberwachung in Echtzeit möglich: Statistische Daten zum Gerätezugriff werden mit Hilfe informativer Diagramme angezeigt. Der aktuelle Status von Agenten ist jederzeit überprüfbar. Wird ein unerwünschtes Gerät mit einem Netzwerkrechner verbunden, kann zudem eine Administratorwarnung verschickt werden. Eine oder mehrere Personen lassen sich hierbei per E-Mail, Netzwerknachricht oder SMS (über einen E-Mail-zu-SMS-Gateway/Dienst) benachrichtigen.

## ■ Umfassende Berichte zur Verwendung mobiler Speichermedien mit dem Zusatzmodul GFI ReportPack

Das GFI EndPointSecurity ReportPack ist ein vollständig integrierbares, umfassendes Reporting-Modul für GFI EndPointSecurity. Mit dem ReportPack können die von GFI EndPointSecurity erfassten Daten automatisch und nach Zeitplan in Form von aussagekräftigen IT- und Management-Berichten ausgegeben werden. So bleiben Sie über mit dem Netzwerk verbundene Geräte informiert und erhalten unter anderem Daten zur Benutzeraktivität. Auch über mobile Hardware ausgetauschte Dokumente werden inklusive ihrer Dateinamen angezeigt.

## ■ Einfache Installation der Agenten zur Zugriffskontrolle im Hintergrund

Agenten können nach der Aktualisierung einer Schutzrichtlinie und anderer Einstellungen automatisch nach Zeitplan auf Netzwerkrechnern bereitgestellt werden. Bei Nichterreichbarkeit eines zu überwachenden Computers erfolgen ohne Administratoreingriff weitere Versuche, bis die Bereitstellung erfolgreich ist. Agenten können vom Remote-Deployment-Tool von GFI EndPointSecurity innerhalb weniger Minuten auf allen Netzwerkrechnern installiert werden. Zudem lassen sich MSI-Dateien für Schutzrichtlinien erstellen und über Active Directory bereitstellen.

### ■ Zeitlich begrenzter Gerätezugriff

Administratoren haben die Möglichkeit, den Zugriff auf ein üblicherweise gesperrtes tragbares Gerät oder eine Gerätegruppe zeitlich begrenzt zu gestatten. Diese für Einzelrechner erteilte Freigabe kann sogar erfolgen, wenn der Agent keine Verbindung mit dem Netzwerk hält.

### ■ Weitere Leistungsmerkmale

- Erlaubt die Suche und Identifizierung von vor Kurzem oder aktuell verwendeten Geräten
- Ermöglicht die Festlegung eines Passworts zum Schutz von Agenten vor Manipulation
- Bietet individuell anpassbare Popup-Meldungen für Gerätesperrungen
- Unterstützt Backend-Datenbank zur Sicherung und Anzeige von Benutzeraktivitäten und Geräteverwendung
- Liefert Wartungsfunktion zum Löschen älterer Daten
- Läuft unter allen Unicode-kompatiblen Betriebssystemen

### ■ Sie befinden sich in guter Gesellschaft ...

Viele führende Unternehmen haben sich bereits für GFI EndPointSecurity entschieden, unter anderem: Best Western Sterling Inn, Fair Trades Ltd, Central Highlands Water, Aurum Funds und viele mehr.

## Systemanforderungen

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

## Auszeichnungen



Ihre Testversion steht unter <http://www.gfi.com/de/endpointsecurity/> zum Download bereit!

GFI Software  
Magna House, 18 – 32 London Road  
Staines, Middlesex  
TW18 4BP  
UK  
Tel +44 (0) 870 770 5370  
Fax +44 (0) 870 770 5377  
sales@gfi.co.uk

GFI Software  
15300 Weston Parkway  
Suite 104  
Cary, NC 27513  
USA  
Tel +1 (888) 243-4329  
Fax +1 (919) 379-3402  
sales@gfiusa.com

GFI Asia Pacific Pty Ltd  
83 King William Road  
Unley 5061  
South Australia  
Tel +61 8 8273 3000  
Fax +61 8 8273 3099  
sales@gfiap.com

GFI Software  
GFI House  
San Andrea Street  
San Gwann SGN 1612  
Malta  
Tel +356 21 382418  
Fax +356 21 382419  
sales@gfi.com

**Microsoft**  
GOLD CERTIFIED  
Partner

**GFI**  
www.gfi.com