Uncontrolled use of USB sticks, MP3 players and PDAs opens up your network to data theft and viruses

Powerful and **user-friendly**

Excellent performance

Comprehensive **control**

Competitive pricing

Available as **FREEWARE**

Comprehensive control on use of iPods, USB sticks and other portable devices

The proliferation of consumer devices such as iPods, USB sticks, smartphones and other portable devices has increased the risk of data leakage and malicious activity on networks. While most companies have antivirus, firewalls, and email and web content security to protect against external threats, few realize how easy it is for an employee to copy huge amounts of confidential and commercially-sensitive data onto an iPod or USB stick without anybody knowing. There is also a high risk of viruses, malware and illegal software being introduced on the network. A draconian way to prevent this from happening is to lock down all USB ports, but this is neither sustainable nor feasible.

BENEFITS

- Prevents data leakage/theft by controlling access to portable storage devices with minimal administrative effort
- Prevents accidental data loss when removable storage devices get lost or stolen by the use of encryption
- Assesses the data leakage risk posed by removable devices at endpoint level and provides information on how to mitigate it
- Controls data transfers involving removable storage devices based on the real file type and contents
- Prevents introduction of malware and unauthorized software on the network
- Protects data on the move with removable volume encryption
- Enables administrators to block devices by class, file extensions, physical port or device ID
- Allows administrators to grant temporary device or port access for a stipulated timeframe
- Can automatically download and install SQL Express if a database server is not available.

GFI EndPointSecurity™

Control of USB sticks, iPods and other endpoint devices

Prevent internal data theft and malware infection

Unfortunately, many businesses ignore or are unaware of the threat until something actually happens. According to research conducted by eMedia on behalf of GFI in the US, few medium-sized businesses consider portable storage devices to be a major threat while less than 20% had implemented software to address this risk. The key to managing portable device use is to install an endpoint security solution that gives administrators control over what devices are in use, have been used and by whom, as well as an in-depth knowledge of what data has been copied. It is also important to control sensitive data when it needs to be taken outside the company's premises on a portable device.

Control portable device use on your network

GFI EndPointSecurity™ enables administrators to actively manage user access and log the activity of:

- Media players, including iPods, Creative Zen and others
- USB sticks, CompactFlash, memory cards, CDs, floppies and other portable storage devices
- iPhone and BlackBerry handhelds, mobile phones, smartphones and similar communication devices
- Network cards, laptops and other network connections.

How it works

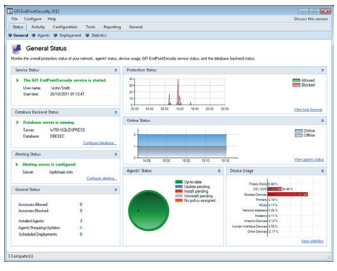
To control access, GFI EndPointSecurity installs a hidden, small footprint agent on the machine. This agent can be deployed to machines network-wide with just a few clicks.

Manage user access and protect your network against the threats posed by portable storage media

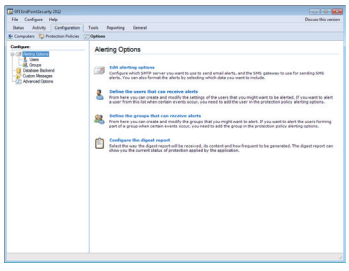
Using GFI EndPointSecurity you can centrally disable users from accessing portable storage media, preventing users from stealing data or bringing in data that could be harmful to your network, such as viruses, trojans and other malware. Although you can switch off portable storage devices such as CD and/or floppy access from the BIOS, in reality this solution is impractical: You would have to physically visit the machine to temporarily switch off protection and install software. In addition, advanced users can hack the BIOS. GFI EndPointSecurity allows you to take control over a wide variety of devices.

Log the activity of portable device access to your network

In addition to blocking access to portable storage media, GFI EndPointSecurity logs device-related user activity to both the event log and to a central SQL Server. A list of files that have been accessed on a given device is recorded every time an authorised user plugs in.



GFI EndPointSecurity Management Console



GFI EndPointSecurity configuration options

Encrypt portable devices

Users can be given permission to store data on USB devices as long as it is encrypted. Access to this data outside the company network can be strictly controlled by a purpose-built traveler application, which is included with GFI EndPointSecurity.

Data aware control of files transiting endpoints via removable devices

Along with real file type detection, GFI EndPointSecurity also delivers content verification based on regular expressions or dictionary files. This enables the detection of security- sensitive information present in popular document formats. The product ships with a number of predefined templates that detect potential leaks of credit card numbers, personal identification numbers and so on.

Other features:

- Centralizes network monitoring, detects connected devices and performs various related tasks
- Policy creation wizard
- Daily/weekly digest
- Automatically protects newly detected computers
- Can automatically download and install SQL Express if a database server is not available
- Advanced granular access control, whitelists and blacklists
- Real-time status monitoring and real-time alerts
- Full reports on device usage with the GFI ReportPack add-on
- Easy unattended agent deployment
- Permits temporary device access
- Scans and detects a list of devices that have been used or are currently still in use
- Password-protected agents avoid tampering; and provides Windows 7 support of tamper-proof agent
- Supports Windows 7 Bitlocker To Go
- Sends users custom popup messages when they are blocked from using a device
- Enables the browsing of user activity and device usage logs through a backend database
- Maintenance function allows administrators to delete information that is older than a certain number of days
- Can group computers by department, by domain, etc.
- Supports operating systems in any Unicode-compliant language
- And more!

System requirements

- Operating system: Windows 2000 (SP4), XP, 2003, Vista, 7 and 2008, Windows 8 and 2012 Server (x86 and x64 versions)
- Internet Explorer 5.5 or later
- .NET Framework version 4.0
- Port: TCP port 1116 (default)
- Database backend: SQL Server 2000/2005/2008; if this is not available, GFI EndPointSecurity can automatically download, install and configure a version of SQL Server Express.

Download your free trial from http://www.gfi.com/endpointsecurity

Microsoft Partner
Gold Independent Software Vendor (ISV)

GFI EndPointSecurity™

Control of USB sticks, iPods and other endpoint devices

Contact us

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

Asia Pacific - South Australia
Tel: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfiap.com

For more GFI offices please visit http://www.gfi.com/company/contact.html

GFI
www.gfi.com