Software available in the following languages

Microsoft GOLD CERTIFIED Partner

GFI EndPointSecurity™

Disclaimers now available for FREE

Control of iPods, USB sticks and other endpoint devices

- Powerful and user-friendly
- Excellent performance
- Comprehensive control
- Unbeatable pricing

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

The proliferation of consumer devices such as iPods, USB drivers, smart phones and other portable devices has increased the risk of data leakage and malicious activity on networks. While most companies have anti-virus software, firewalls, 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 advised.

Compatible with Windows 7

CERTIFIED FOR Windows Server 2008 R2

BENEFITS

- **Prevents data leakage/theft by comprehensively controlling access to portable storage devices with minimal administrative effort**
- **Prevents introduction of malware and unauthorized software on the network**
- **Gives administrators greater control by enabling them 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**
- **Support for 32 & 64-bit platforms: Including Windows 7, Vista and latest RC of Windows Server 2008.**

Business Solutions BEST CHANNEL PRODUCT 2009

Window Security.com Gold Award ★★★★

TMC LABS INNOVATION 2006 AWARD

Prevent data theft and virus infection from within with endpoint security software

Unfortunately, many businesses are unaware of or ignore 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 fewer 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 and in-depth knowledge of what data has been copied.

Control portable device use on your network with GFI EndPointSecurity™

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

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

How it works

To control access, GFI EndPointSecurity installs a small footprint agent on the machine. This agent is only 1.2 MB in size – the user will never know it is there. GFI EndPointSecurity includes a remote deployment tool based on GFI LANguard technology, allowing you to deploy the agent to hundreds of machines with just a few clicks. After installation, the agent queries Active Directory when the user logs on and sets permissions to the different nodes accordingly. If the user is not a member of a group that allows him/her access, then access to the device is blocked.

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

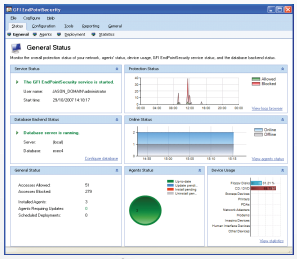
Using GFI EndPointSecurity you can centrally disable users from accessing portable storage media preventing users from stealing data or bringing in data that could be harmful to your network, such as viruses, trojans and other malware. Although you can switch off portable storage devices such as CD and/or 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

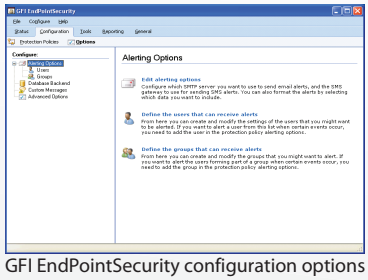
In addition to blocking access to portable storage media, GFI EndPointSecurity logs device-related user activity to both the event log and to a central SQL Server. A list of files that have been accessed on a given device is recorded every time an allowed user plugs in.

Other features:

- Advanced granular access control, whitelists and blacklists
- Real-time status monitoring and real-time alerts
- Get full reports on device usage with the GFI ReportPack add-on
- Easy unattended agent deployment
- Temporary device access
- Scan and detect a list of devices that have been used or are currently still in use
- Password-protected agents to avoid tampering and Windows 7 support of Tamperproof agent
- Support for Windows 7 Bitlocker To Go
- Set up custom popup messages for users when they are blocked from using a device
- Browse user activity and device usage logs through a backend database
- Maintenance function that allows you to delete information that is older than a certain number of days
- Support for operating systems in any Unicode-compliant language
- And more!



GFI EndPointSecurity Management Console



GFI EndPointSecurity configuration options

System requirements

- Operating system: Windows 2000 (SP4), XP, 2003, Vista, 7 and 2008 (x86 and x64 versions)
- Internet Explorer 5.5 or later
- .NET Framework version 2.0
- Database Backend: SQL Server 2000, 2005, 2008
- Port: TCP port 1116 (default).

For more information and to download your free evaluation version please visit http://www.gfi.com/endpointsecurity/

Microsoft GOLD CERTIFIED Partner

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

Australia - Asia Pacific
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.htm

www.gfi.com