Comprehensive control on use of USB storage and other portable devices

The proliferation of consumer devices such as smartphones, media players, portable storage devices, network connected devices and easily concealable USB sticks has increased the risk of data leakage, virus infection, introduction of un-licenced software and games and other 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 a portable storage device without anybody knowing.

Physically locking down all USB ports, is neither sustainable nor feasible. 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.

How it works

To control access, GFI EndPointSecurity automatically installs a tamper-proof, hidden agent on the machines in your network. This agent can be deployed to machines network-wide with just a few clicks. This agent delivers unparalleled tamper protection even against users with admin rights, enabling IT admins to remain in control no matter what.

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

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. Although you can switch off some physical connection ports from the BIOS, in reality this solution is impractical and advanced users can hack the BIOS with ease. 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 authorized device is plugged-in.

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.

Other features:

- Policy creation wizard for advanced granular access control
- Daily/weekly digest
- Real-time status monitoring and real-time alerts
- Full reports on device usage with the GFI ReportPack add-on
- 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
- Can group computers by department, by domain, etc.
- Supports operating systems in any Unicode-compliant language
- And more!

Benefits at a glance

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

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

For a full list of benefits visit: **www.gfi.com/endpointsecurity**

System requirements

Windows 2000 (SP4), XP, Vista, 7, and 8, Windows Servers 8 and 2012 (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.

GFI®

www.gfi.com

For a full list of GFI offices/contact details worldwide, please visit: www.gfi.com/contact-us