

“Highest Performance  
Lowest Price”

**Microsoft**  
GOLD CERTIFIED  
Partner

# GFI EndPointSecurity

Сетевой контроль за iPod, USB-накопителями и другими переносимыми устройствами

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

## Управление доступом к переносимым устройствам хранения информации, таким как USB-накопители, iPod и PDA

Вы вложили средства в сетевое антивирусное программное обеспечение, системы сетевой защиты, безопасность электронной почты и веб-содержимого для защиты от внешних угроз. И все же любой пользователь может войти в офис, подключить USB-устройство размером с брелок для ключей и ввести/вывести более 80 Гб данных. В этом может заключаться большая угроза: пользователи могут скопировать секретные данные или бессознательно ввести вирусы, трояны, незаконное программное обеспечение и др. – действия, которые могут отразиться на работоспособности вашей сети и компании в целом. Кроме того, как администратор вы никак не можете контролировать это! Групповая политика не предлагает никакого управления, а полная блокировка портов USB – это нерациональное решение.

### ПРЕИМУЩЕСТВА



- Блокирует похищение данных с помощью полностью управляемого доступа к портативным запоминающим устройствам, таким как карты памяти, компакт-диски, USB-накопители и др.
- Предотвращает попадание вирусов и незаконного программного обеспечения с помощью управления всеми подключаемыми к конечной точке устройствами, например, PDA, ноутбуки и др.
- Позволяет администраторам осуществлять управление на групповой основе по широкому ряду портативных устройств, не затрагивая авторизованных пользователей
- Предотвращает потерю производительности, блокируя несанкционированные загрузки игр и других персональных файлов из портативных запоминающих устройств
- Поставляется с тремя политиками защиты: для ноутбуков, рабочих станций и серверов.



## Предотвратите утечку данных и заражение вирусами изнутри сети с помощью специализированного программного обеспечения

Согласно исследованию компьютерной преступности ФБР 2005 года 44% организаций сообщили о сетевых вторжениях изнутри своих организаций. Аналитики компании Gartner предупреждают, что портативные устройства, имеющие USB- или FireWire- подключение являются новой серьезной угрозой организациям. В своем отчете Gartner назвали портативные запоминающие устройства серьезной угрозой безопасности рабочих станций и сообщили, что они могут использоваться как для загрузки конфиденциальной информации, так и ввести вирус в сеть компании.

## Восстановите контроль над сетью с помощью GFI EndPointSecurity

GFI EndPointSecurity позволяет администраторам управлять доступом пользователей и регистрировать активность:

- Медиплееров, включая iPod, Creative Zen и др.
- USB-накопителей, CompactFlash, карт памяти, компакт-дисков, дисководов и других портативных запоминающих устройств
- Портативных устройств PDA, BlackBerry, iPhone мобильных телефонов и подобных устройств связи
- Сетевых карт, ноутбуков и других сетевых подключений

### Принцип работы

Для управления доступом система GFI EndPointSecurity устанавливает на машину небольшой агент. Агент занимает всего 1,2 Мб, пользователь не будет подозревать об его присутствии. GFI EndPointSecurity использует инструмент удаленного развертывания, основанный на технологии GFI LANguard, позволяющий разместить агент на сотнях машин несколькими нажатиями клавиш. После установки при входе пользователя в систему агент обращается Active Directory и устанавливает соответствующие полномочия по различным узлам. Если пользователь не является членом группы, разрешающей доступ, доступ к устройству блокируется.

## Управляйте пользовательским доступом и защитите свою сеть от угроз, которые могут возникнуть из-за использования переносимых устройств хранения данных

Используя GFI EndPointSecurity, можно централизованно блокировать доступ пользователя к переносимому устройству хранения данных, обеспечивая защиту от похищения

информации или внесения данных, потенциально опасных для сети организации, например, вирусов, троянцев и других вредоносных программ. Хотя переносимые устройства хранения информации, такие как CD-ROM или накопители на гибких дисках, можно отключить через BIOS, такое решение непрактично: для этого необходим физический доступ к машине. Кроме этого, опытные пользователи могут отключить защиту через BIOS. Решение GFI EndPointSecurity позволяет взять в свои руки управление различными видами устройств, включая:

- Накопители на гибких дисках;
- CD и DVD-ROM;
- iPod;
- Устройства хранения данных;
- Принтеры;
- PDA;
- Сетевые адаптеры;
- Модемы;
- Устройства передачи изображений;
- И так далее!

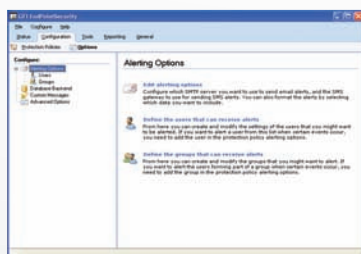


## Регистрируйте активность переносимых устройств хранения данных, таких как карты памяти USB, SD-карты и т.д.

Карты памяти USB являются одной из основных угроз, поскольку они небольшие, их легко спрятать, и они хранят до 4 Гб данных. Например, подключение цифровой камеры к порту USB предоставляет пользователю возможность сохранения информации на SD-карте; SD-карты могут иметь самый различный объем, включая 2 Гб и более. Кроме этого, для блокирования доступа к переносимым устройствам хранения данных в GFI EndPointSecurity регистрируется пользовательская активность по отношению к устройству, как в журнал регистрации событий, так и в центральный сервер SQL. При подключении пользователем устройства к сети регистрируется список файлов, к которым был получен доступ и которые были переданы с устройства или на него.



Панель управления GFI EndPointSecurity



Настройки GFI EndPointSecurity

## Системные требования

- ОС: Windows 2000 (SP4), XP, 2003, Vista и 2008 (x86 и x64 версии)
- Internet Explorer 5.5 и более новые
- .NET Framework 2.0
- SQL Server 2000, 2005, 2008
- Порт: TCP port 1116 (по умолчанию)



Для получения более подробной информации и бесплатной демонстрационной версии продукта, пожалуйста посетите <http://www.gfi.ru>

Генеральный дистрибьютор GFI в России и СНГ:

**CONTROL  
LINE**

117574, Москва, Одоевского, 7-2-240  
+7 (495) 799-1920  
[www.gfi.ru](http://www.gfi.ru)  
[info@gfi.ru](mailto:info@gfi.ru)