"Highest Performance
Lowest Price"

GFI

EndPointSecurity

План

- Установка
- Размещение агентов
- Как агент EndPointSecurity Agent защищает компьютер
- Ведение журнала
- EndPointSecurity и BSOD
- Как удалить EndPointSecurity Agent вручную

Установка (1/3)

- GFI EndPointSecurity (ESEC) поддерживает Windows 2000/2003/2008, Windows XP Pro и Vista
- Доступны версии для 32-bit и 64-bit
- ESEC может быть использован как в условиях Active Directory (AD), так и в окружении рабочей группы
- В AD, ESEC создаст AD группы для того, чтобы предоставить возможность моментальной настройки прав для пользователей

Установка (2/3)

- Использование AD позволяет настроить права без обновления агентов на конечных компьютерах
- Изменения будут применены как только настройки AD будут обновлены на конечных машинах
- AD Domain Controller гарантированно обновляет настройки после следующего захода пользователя в систему
- Если Вы хотите настраивать работу ESEC через интерфейс продукта, помните, что для применения изменений должны будут быть обновлены все установленные агенты на конечных компьютерах

Установка (3/3)

- В условиях отсутствия AD администратор имеет возможность настраивать права только через интерфейс программы
- ESEC создаст группы доступа на локальных машинах, но не глобально
- Есть возможность сопряжения AD и неподключенных к AD компьютеров
- Когда Вы настраиваете пользователя в домене, он будет отображен как <domain\user>

Размещение агентов

- Следующие условия необходимы для размещения агентов
  - Включенная настройка "File and Printing sharing"
  - Открытые порты 1070-1170
  - TCP port 1323
    - Используется для ведения журнала в SQL server
  - TCP Port 1116
    - Используется для передачи статуса GFI EndPointSecurity server.
  - Доступ к Remote Registry Service

Как агент EndPointSecurity Agent защищает компьютер

- ESEC Agent состоит из 3 модулей:
  - GFI EndPointSecurity Agent service
    - Отвечает за ограничение доступа к устройствам
  - ESEC driver – epsdrv.sys, <system32\drivers>
    - Перехватывает обращения к подключенным устройствам компьютера
  - Agent Logger
    - Ведет журнал событий для возможной отладки

Ведение журнала

- ESEC предоставляет два варианта ведения журнала: Event Log и SQL БД
- Может быть записано любое событие, связанное с работой продукта
- В случае использования Event Log, событие будет размещено на защищаемой машине

EndPointSecurity и BSOD

- ESEC Agent Device Driver работает на нижнем уровне ОС
- Появление ошибки в драйвере может вызывать BSOD
- Эти проблемы должны быть решены сразу же после появления, иначе работоспособность продукта будет нарушена

Как удалить EndPointSecurity Agent вручную (1/2)

- Бывают случаи, когда необходимо удалить ESEC агента вручную
- Запустите машину с установочного диска Windows (используя ту же версию Windows, что и установленная)
- Выберите вариант восстановления системы через Recovery Console
- В Recovery Console перейдите в папку Windows

Как удалить EndPointSecurity Agent вручную (2/2)

- Введите логин/пароль администратора
- Пройдите в system32\drivers
- Удалите файл драйвера командой 'del epsdrv.sys'
- Введите 'exit' для перезагрузки машины

“Highest Performance
Lowest Price”

GFI

EndPointSecurity

Вопросы?