

# **GFI LanGuard**<sup>TM</sup>

Управление сетевыми уязвимостями

## **Три основных компонента управления безопасностью**

GFI LANguard – это комплексное решение, позволяющее сканировать, обнаруживать, оценивать и устранять уязвимости в сети. Как администратор, вам часто приходится сталкиваться с проблемами, связанными с вопросами уязвимости сети, управлением обновлениями и патчами и сетевым аудитом при использовании различных продуктов. GFI LANguard объединяет эти три компонента управления безопасностью в один пакет. Используя единую консоль с обширными функциональными возможностями по созданию отчетов, решение GFI LANguard позволяет справиться с этими проблемами быстро и эффективно

### **ПРЕИМУЩЕСТВА**

- База в более чем 15 000 потенциальных уязвимостей сети
- Снижение расходов благодаря объединенному решению для поиска уязвимостей, управления обновлениями и патчами и сетевого аудита
- Создание различных отчетов по сканированию, выполненному по всей сети, включая приложения и ресурсы
- Сетевой администратор способен защитить сеть быстро и эффективно
- Предотвращение «падения» серверов и сети благодаря своевременному обнаружению уязвимостей
- Лучший коммерчески доступный сканер безопасности Windows (по мнению пользователей Nmap, использующих его в течение двух лет).



### Интегрированное решение по управлению защитой

GFI LANguard – это комплексное решение, использующее для защиты три основных компонента: сканер безопасности, управление внесением исправлений и сетевой аудит с помощью одной объединенной консоли. Просматривая всю сеть, он определяет все возможные проблемы безопасности и, используя свои обширные функциональные возможности по созданию отчетов, предоставляет средства, необходимые для обнаружения, оценки, описания и устранения любых угроз.

- Проверка уязвимости
- Управление внесением исправлений
- Сетевой и программный контроль

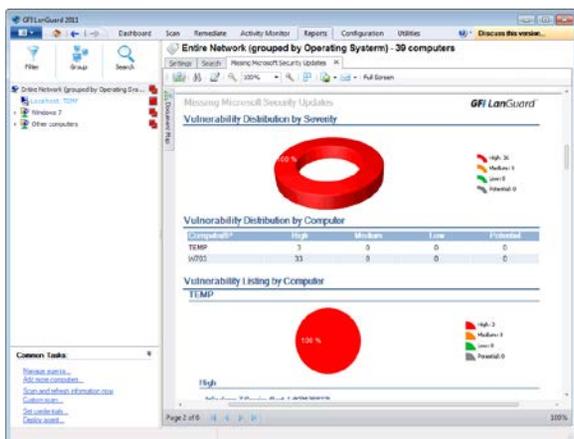
### Сканер безопасности и управление внесением исправлений

Лучший коммерчески доступный сканер безопасности по мнению пользователей Nmap, использующих его в течение двух лет, и победитель в категории Patch Management в номинации TechTarget 2006 «Products of the Year», GFI LANguard является наиболее полным решением по управлению безопасностью в одном пакете. GFI LANguard 9 – это эффективное, недорогое решение для организаций, которым необходима защита своих сетей и систем от хакерских атак и угроз безопасности.

### Проверка на уязвимости

В процессе проверки безопасности производится более 15 000 оценок на уязвимость, а в сети проверяется каждый IP-адрес. GFI LANguard предоставляет возможность выполнения многоплатформенного сканирования (Windows, Mac OS, Linux) и анализирует состояние сети по каждому источнику данных. Это обеспечивает возможность идентификации и устранения любых угроз прежде, чем хакеры добьются своего.

- Определение угроз безопасности и выполнение корректирующих действий
- база данных уязвимостей
- Определение устаревших антивирусных баз ведущих производителей антивирусной защиты
- Простота создания различных типов тестов на уязвимость
- Создание собственных схем проверки на уязвимость
- Простой анализ и фильтрация результатов сканирования



### Поддержка нескольких баз данных и автоматического управления ими

Существует возможность хранения электронной почты в нескольких базах данных – это устраняет проблему использования одной крупной базы, которая становится со временем медленной и требует больших затрат на ее По завершении сканирования GFI LANguard предоставляет вам все возможности и средства для эффективной установки обновлений и патчей на всех машинах с различными операционными системами. С помощью GFI LANguard вы сможете скачать и установить отсутствующие обновления от Microsoft в автоматической режиме. Используя GFI LANguard можно также устанавливать программное обеспечение других производителей.

- Автоматическая установка исправлений и пакетов обновлений
- Развертывание стороннего программного обеспечения и исправлений в сети

### Сетевой и программный аудит

Функция аудита GFI LANguard предоставляет вам всю необходимую информацию о вашей о сети – подключенные USB-устройства, установленное программное обеспечение, открытые для общего доступа файлы, открытые порты и слабые пароли. Возможность создания детальных отчетов отображает состояние сети в режиме реального времени. Результаты просмотра можно легко проанализировать с помощью фильтров и отчетов, обеспечивая проактивную защиту сети закрытием портов, удалением неиспользуемых учетных записей пользователей или групп, отключением точек беспроводного доступа и т.д.

### Автоматическое уведомление о новых потенциальных уязвимостях

GFI LANguard может выполнять запланированное сканирование (например, ежедневно или еженедельно) и автоматически сравнивать результаты с предыдущими проверками. Вы будете проинформированы обо всех обнаруженных уязвимостях в защите или изменениях параметров безопасности в сети. Это позволяет вам быстро обнаруживать недавно созданные ресурсы, установленные службы, приложения, добавленных пользователей, недавно открытые порты и др.

### Другие возможности

- Мощная система создания отчетов GFI LANguard ReportPack
- Соответствие PCI DSS и другим стандартам
- Предварительно настроенные параметры для различных проверок

### Системные требования

- Windows 2000 (SP4), XP (SP2), 2003, 2008, VISTA, 7
- Internet Explorer 5.1 или выше.
- Client for Microsoft Networks component – включен в ОС Windows 95 и выше.
- Secure Shell (SSH) – включен в каждый дистрибутив Linux по умолчанию.

Получить информацию о продукте, загрузить демонстрационную версия, рассчитать стоимость и узнать о действующих скидках и специальных акциях Вы можете на сайте <http://www.gfi.ru/>

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@gfi.com

Россия и СНГ  
Tel +7(495)799 1920  
Fax +7(495)422 9933  
info@gfi.ru

