

“Highest Performance
Lowest Price”

Microsoft
GOLD CERTIFIED
Partner

GFI MailSecurity

Защита от вирусов и троянов, политика использования
содержимого, обнаружение вторжений

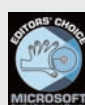
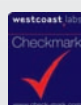
- **No. 1** multiple AV email security product
- Over **30,000** customers
- Unbeatable pricing
- Outstanding security performance

Антивирусное программное обеспечение, защищающее от вирусов, троянов и вторжений

Необходимость проверки сообщений электронной почты на опасное, вредоносное или конфиденциальное содержимое никогда не было таким очевидным. Наиболее опасные вирусы, способные вывести из строя почтовый сервер и корпоративную сеть в считанные минуты, распространяются по всему миру посредством электронной почты, и это вопрос нескольких часов. Обычные продукты, которые выполняют только антивирусное сканирование, не обеспечивают достаточную защиту. Хуже всего то, что электронная почта стала средством создания лазеек (троянов) и других вредоносных программ, помогающих проникнуть в сеть. Продукты, ограниченные одним антивирусным механизмом, не способны к защите от атак подобного вида.

ПРЕИМУЩЕСТВА

- **Поддержка ведущих платформ для сообщений, включая Microsoft Exchange 2000, 2003 и 2007**
- **Множественные антивирусные механизмы гарантируют более высокий уровень обнаружения и более быстрый отклик**
- **Уникальный сканер обнаруживает вредоносные исполняемые файлы без необходимости в обновлениях – MyDoom был обнаружен мгновенно!**
- **Механизмы обнаружения вторжений и активного содержимого HTML отключают HTML-сценарии и предотвращают вторжения.**



Зачем нужно использовать несколько антивирусных механизмов

Исследования показывают, что различные антивирусные механизмы имеют сильно отличающиеся времена отклика для новейшей угрозы. Зависимость от антивирусного механизма, который отвечает на новую угрозу через 9 часов вместо того, чтобы делать это немедленно, значительно увеличивает шансы заражения.

Кроме этого, ни один антивирусный механизм не способен полностью защитить от всех возможных угроз: каждый сканер имеет свои сильные и слабые стороны. Например, после появления вируса MyDoom одни производители быстрее других выпустили образы этого вируса. Это различие – вопрос нескольких часов; пока многие его обнаружат для заражения сети пройдет более чем достаточно времени.

Учитывая неспособность отдельного антивирусного механизма быстро отвечать и обеспечивать полный охват всех почтовых атак, логика подсказывает, что объединение нескольких механизмов обеспечит более полное решение. Простыми словами, если антивирусные продукты X и Y – каждый сильнее в одной области и слабее в другой – используются совместно, их объединенная сила с большей вероятностью охватит более широкий диапазон угроз, и, таким образом, нейтрализует слабые стороны друг друга. Наличие нескольких сканеров на уровне почтового сервера компенсирует различия во времени отклика разных антивирусных механизмов и сократит среднее время отклика, что значительно снизит шанс заражения.

Использование нескольких антивирусных механизмов также дает возможность администраторам быть не зависящими от производителя продукта, когда дело касается сканирования вирусов, позволяя использовать лучшие из механизмов, доступных на рынке.



Настройка проверки прикрепленных файлов



Настройка GFI MailSecurity



Зачем нужно использовать анализатор исполняемых файлов и троянов

Новейший вирус Novarg, возможно, лучше всего продемонстрирует, зачем нужно использовать анализатор исполняемых файлов и троянов: из-за характеристик этого вируса GFI MailSecurity обнаружил, что он является вредоносным исполняемым файлом без необходимости в обновлении базы данных подписей вирусов. Пока поставщики антивирусных баз подготовят и распределят обновления для обнаружения Novarg, пользователи GFI MailSecurity уже будут защищены от него. Чтобы обновить и распределить файлы образа, может пройти несколько часов, а это может быть слишком поздно для вашей сети!

Различие между антивирусным механизмом и сканером троянов и исполняемых файлов

Поскольку антивирусное программное обеспечение основано на образе вируса, оно может обнаруживать только известные вирусы и трояны, и неспособно обнаруживать новые вирусы, типа Novarg без новых файлов образа. Сканер троянов и исполняемых файлов GFI MailSecurity использует другой подход: Вместо того, чтобы полагаться на подпись, он использует патентованный, встроенный интеллект для оценки риска исполняемых файлов. Он делает это дизассемблированием исполняемого файла, обнаруживая в режиме реального времени, что он мог бы сделать, и сравнивая его действия с базой данных вредоносных действий. Таким образом, GFI MailSecurity способен обнаруживать неизвестные вирусы и трояны прежде, чем они попадут в сеть, и прежде, чем поставщики антивирусных механизмов выпустят соответствующие обновления. Используя эту методику, GFI MailSecurity может также обнаружить одноразовые трояны или вредоносные программы – направленные на определенного пользователя, чтобы получить определенную информацию. Поскольку эти угрозы – одноразовые, антивирусное программное обеспечение никогда не распознает их.

Системные требования

- Windows 2000 Server/Advanced Server (Service Pack 1 и выше) или Windows 2003 Server/Advanced Server или Windows XP
- Microsoft Exchange server 2000 (SP1), 2003, 2007, 4, 5 или 5.5, Lotus Domino, или любой другой SMTP/POP3 почтовый сервер
- При использовании Small Business Server, убедитесь в том, что установлены SP 2 для Exchange Server 2000 и SP1 для Exchange Server 2003
- Microsoft .NET Framework 1.1/2.0
- MSMQ - Microsoft Messaging Queuing Service
- Internet Information Services (IIS) - SMTP service & World Wide Web service
- Microsoft Data Access Components (MDAC) 2.8.

↓ 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
info@gfi.ru