GFI MailSecurity™

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

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, 2007 и 2010**
- **Множественные антивирусные механизмы гарантируют более высокий уровень обнаружения и более быстрый отклик**
- **Уникальный сканер обнаруживает вредоносные исполняемый файлы без необходимости в обновлениях – MyDoom был обнаружен мгновенно!**
- **Механизмы обнаружения вторжений и активного содержимого HTML отключают HTML-сценарии и предотвращают вторжения.**

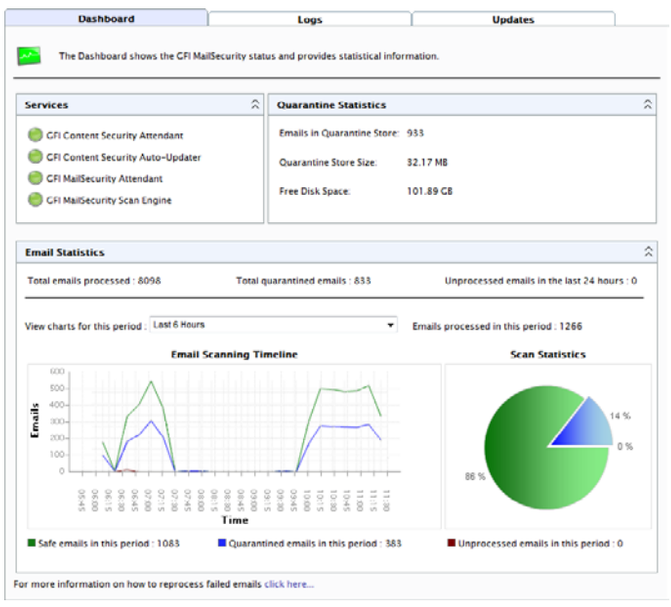
Зачем нужно использовать несколько антивирусных механизмов

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 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 оклика 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.



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, Windows Server 2008 или Windows XP
- Microsoft Exchange server 2000 (SP1), 2003, 2007, 2010, 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.

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