

Получите 14 фильтров защиты от спама, 3 антивирусных ядра и сканирование на наличие вредоносных программ в одном пакете защиты электронной почты

Ежедневно отправляются и получаются миллиарды электронных писем, поэтому электронная почта часто становится средством взлома вашей организации. GFI MailEssentials прост в использовании и предлагает полный набор средств защиты вашей компании и повышения производительности электронной почты.

- ✓ **Блокируйте вирусы и вредоносное ПО, передаваемые по электронной почте** - Зачем доверять защиту электронной почты одному антивирусному ядру, если у вас есть комбинация из трех возможностей? GFI MailEssentials может использовать возможности ведущих брендов, включая BitDefender, Avira и Sophos. Каждое ядро имеет свои собственные эвристические алгоритмы и методы обнаружения. Вы получаете максимальную защиту своей электронной почты, чтобы более эффективно блокировать вирусы, передаваемые по электронной почте, и другие вредоносные программы.
- ✓ **Фильтрация спама и обнаружение фишинговых атак** - Отфильтровывайте спам до того, как он попадет в почтовые ящики, чтобы сэкономить место на сервере и продуктивное время. GFI MailEssentials использует 14 передовых технологий фильтрации электронной почты, которые вы можете увидеть в действии. Модуль защиты от фишинга GFI MailEssentials обнаруживает и блокирует угрозы, исходящие от фишинговых писем, путём сравнения содержимого спама с постоянно обновляемой базой данных и фишинговыми URL-адресами.
- ✓ **Сделайте электронную почту безопасной и продуктивной... просто** - GFI MailEssentials совместим с различными почтовыми серверами, а не только с Exchange. Он легко вписывается в вашу текущую настройку - будь то локальная, виртуальная или размещённая в вашей облачной инфраструктуре. ИТ-администраторы полностью контролируют безопасность своей электронной почты.

До трех антивирусных ядер

GFI MailEssentials поставляется с мощными антивирусными ядрами Avira и BitDefender. Добавьте антивирусный движок Sophos для максимальной защиты. Производители антивирусных ядер имеют разное время реакции на новые вирусы и вредоносные программы. Эта возможность гарантирует, что ваша система всегда сможет обнаруживать новые угрозы в кратчайшие сроки.

Расширенная защита от вредоносных программ

GFI MailEssentials обеспечивает расширенную защиту от вредоносных программ с помощью механизмов сканирования, которые подключаются к облачной службе всякий раз, когда обнаруживают неизвестные выполняемые вложения. Эти вложения тщательно сканируются, чтобы определить, является ли вложение вредоносным.

Арсенал антиспамовых фильтров

GFI MailEssentials поддерживает различные технологии защиты от спама. SPF блокирует поддельные электронные письма. Серый список блокирует электронные письма, отправленные спамерами с использованием методов, не совместимых с RFC. Защита от атак с целью сбора действующих адресов блокирует электронные письма, отправленные с использованием случайных и исчерпывающих методов создания адресов электронной почты. Чёрные списки DNS используют обширную информацию, собранную с помощью методов распределенного сбора данных сообщества, чтобы предотвратить рассылку спама ботнетами.

Веб-консоль со встроенной отчётностью

Вы можете управлять всеми функциями защиты от спама электронной почты, включая карантин спама и вредоносных программ, а также создавать отчёты с единой веб-консоли. Консоль включает в себя информационную панель, которая дает вам графическое представление в реальном времени о состоянии программного обеспечения, а также о потоке электронной почты на сервере.

Управление карантинном

GFI MailEssentials даёт вам возможность выбирать, что делать со спамом и вредоносными сообщениями. Пользователи могут отмечать электронные письма как спам. Вы можете поместить в карантин подозрительный спам и уведомить пользователей. Вы можете установить локацию центрального карантина для вредоносных программ.

Контроль содержания электронной почты и предотвращение утечки данных

Функцию проверки ключевых слов в GFI MailEssentials можно использовать для сканирования входящих и исходящих сообщений электронной почты на предмет ключевых слов, а функция проверки вложений сканирует сообщения электронной почты на наличие вложений.

Вы можете заблокировать все входящие электронные письма с потенциально вредоносными типами вложений или заблокировать потери трафика и производительности, такие как файлы mр3 и mpeg.

Расширенные правила фильтрации электронной почты на основе пользователей позволяют блокировать электронные письма на основе определенных вами шаблонов, таких как регулярные выражения. Это намного эффективнее простой проверки ключевых слов.

Защитите свою компанию от уязвимости электронной почты и троянов

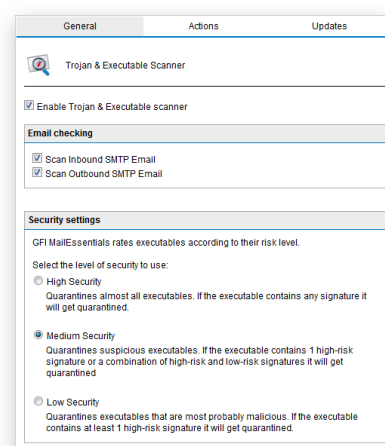
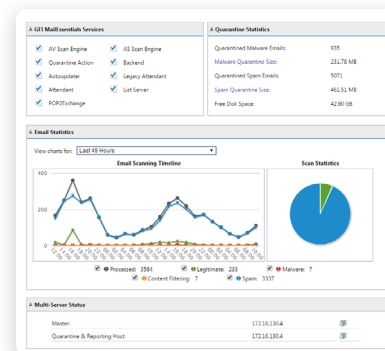
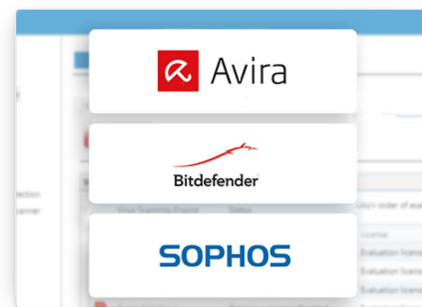
Сканер троянцев и исполняемых файлов GFI MailEssentials обнаруживает неизвестные вредоносные исполняемые файлы, анализируя их действия. Сканер использует встроенный интеллект для оценки уровня риска путём обратного ассемблирования исполняемого файла, определения того, что он может делать, и сравнивая свои действия с базой вредоносных действий. Затем сканер помещает в карантин все исполняемые файлы, которые выполняют подозрительные действия, например, устанавливают сетевые подключения или обращаются к адресной книге.

Защитите своих пользователей от фишинга и шпионского ПО

Модуль защиты от фишинга GFI MailEssentials обнаруживает и блокирует угрозы, исходящие от фишинговых писем, путем сравнения содержимого спама с постоянно обновляемой базой данных и фишинговыми URL. Это обеспечивает сбор всех последних фишинговых писем.

В качестве дополнительной защиты он также проверяет типичные ключевые слова фишинга в каждом электронном письме, отправляемом вашей организацией.

GFI MailEssentials также обнаруживает шпионское ПО, передаваемое по электронной почте, с помощью своего антивирусного ядра, которое включает в себя специальный файл определений шпионского и рекламного ПО, содержащий обширную базу данных известных шпионских программ, троянов и рекламного ПО.



Попробуйте бесплатно в течение 30 дней