Dr.Web для Qbik WinGate

Системные требования

- Место на жестком диске: не менее 50 МБ.
- Операционная система: Microsoft Windows 2000/XP/Vista, Microsoft Windows Server 2000/2003
- Прокси-сервер: Qbik WinGate 6.

Ключевые функции

- Антивирусная и антиспам-проверка почтовых сообщений, передаваемых по протоколам SMTP и POP3, включая проверку вложенных файлов.
- Антивирусная проверка файлов и данных, передаваемых по протоколам HTTP и FTP.
- Лечение инфицированных файлов, передаваемых по протоколу HTTP.
- Возможность сформировать список проверяемых протоколов обмена данными.
- Настраиваемые параметры сканирования: максимальный размер и типы проверяемых объектов, способы обработки инфицированных объектов.
- Возможность включения/отключения детектирования вредоносных программ (по их типам). При обнаружении угроз безопасности к ним применяются действия согласно настройкам Qbik.
- Возможность выбора действий для файлов, не поддающихся проверке.
- Детектирования вредоносных объектов в многократно заархивированных файлах.
- Наличие эффективного и компактного модуля антиспама, что выгодно выделяет Dr.Web для Qbik WinGate среди конкурирующих продуктов.
- Антиспам не требует обучения и позволяет задавать различные действия для разных категорий спамаЧерные и белые списки электронных адресов.
- Возможность выбора действий для различных видов спама, включая перемещение в карантин и добавление префикса к теме письма.
- Регистрация ошибок и происходящих событий в журнале регистрации событий

(Event Log). В журналы заносится информация о параметрах модулей, сообщения об обнаружении вирусов для каждого зараженного письма и для каждого вируса в отдельности (русский и английский языки сообщений).

- Изоляция инфицированных файлов в собственном карантине плагина и/или карантине WinGate.
- Возможность просмотра карантина, восстановления и / или пересылки сохраненных в нем файлов.
- Сохранение в карантине резервных копий вылеченных файлов.
- Собственная панель управления и менеджер карантина.
- Автоматические обновления вирусных баз.

Уникальные возможности ядра

- Проверка архивов любого уровня вложенности.
- Высочайшая точность выявления упакованных вредоносных объектов (даже тех, которые упакованы неизвестным Dr.Web методом), разбор их на компоненты и детальный анализ с целью обнаружения скрытых угроз.
- Детектирование и нейтрализация сложных вирусов, таких как Shadow.based (Conficker), MaosBoot, Rustock.C, Sector – в этом Dr.Web нет равных.
- Интеллектуальные технологии проверки памяти позволяют блокировать активные вирусы до появления их копий на жестком диске компьютера, что снижает вероятность использования вредоносным ПО уязвимостей установленных программ или операционной системы.
- Обнаружение и нейтрализация вирусов, которые действуют в оперативной памяти и никогда не встречаются в виде отдельных файлов (например, Slammer и CodeRed).

Борьба с неизвестными угрозами

- FLY-CODE – не имеющая аналогов технология универсальной распаковки файлов, запакованных неизвестными Dr.Web способами.
- Уникальная технология несигнатурного поиска Origins Tracing™ позволяет Dr.Web с высокой долей вероятности распознавать вирусы, еще не внесенные в вирусную базу.

- Эвристический анализатор Dr.Web эффективно детектирует все распространенные типы угроз, определяя их класс по результатам проведенного разбора и характерным признакам.

Антивирус

Dr.Web для Qbik WinGate обнаруживает инфицированные вложения в электронных письмах, а также зараженные объекты, передаваемые по протоколам HTTP и FTP, в том числе:

- инфицированные архивы;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы.

Dr.Web для Qbik WinGate не проверяет:

- данные, передаваемые по протоколу HTTP в зашифрованном виде (HTTPs);
- зашифрованные почтовые сообщения;
- поврежденные и защищенные паролем архивы.

В случае обнаружения вирусов и других типов вредоносных объектов, а также в случае невозможности проверки объекта к ним применяются действия согласно настройкам программы.

Антиспам

Антиспам позволяет фильтровать электронные сообщения, обрабатываемые службами SMTP server и POP3 proxy server, предотвращая тем самым получение нежелательных

сообщений, например, рекламных рассылок.

Проверка почты на спам производится по трем категориям спама: письма с высокой, средней и низкой вероятностью спама. Для каждой категории можно задать одно из следующих действий:

- **Пропустить** – письмо будет пропущено и доставлено получателю;
- **Переместить в карантин** – письмо будет изолировано в соответствии с настройками карантина и не будет доставлено получателю;

- **Удалить** – письмо будет удалено;
- **Добавить префикс в тему письма и доставить** – в тему письма будет добавлен текст, указанный в поле «Префикс», и письмо будет доставлено получателю.

Для дополнительной фильтрации сообщений используются черный и белый списки. Для писем, пришедших с адресов, добавленных в белый список адреса, не будут применяться никакие действия вне зависимости от их содержания. Если же адрес добавлен в черный список, все письма с этого адреса попадут в категорию Высокая вероятность спама, и к ним будут применены соответствующие действия.

Всегда актуальный

- Процесс обновления происходит незаметно для пользователя — при подключении к сети Интернет, по запросу или по расписанию.
- Загрузка осуществляется быстро (даже на медленных модемных соединениях).
- Всегда имеются доступные серверы обновлений.
- По завершении обновления в большинстве случаев не требуется перезагружать компьютер: Dr.Web сразу готов к работе с использованием самых свежих вирусных баз.

- Обновления отличаются небольшими размерами — в пределах 50–200 КБ.
- Для экономии трафика можно настроить прием только обновлений вирусных баз. Включать эту опцию не рекомендуется. Dr.Web с целью противодействия новым киберугрозам постоянно совершенствуется. Новые возможности включаются в обновленные модули антивирусного пакета и автоматически загружаются с серверов компании при очередном обновлении.

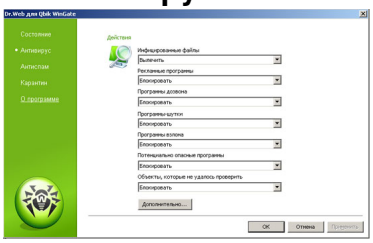
- Скачивать обновления можно в виде заархивированных файлов — тем самым трафик экономится. Для уменьшения размеров скачиваемых обновлений компания «Доктор Веб» использует специальный алгоритм сжатия передаваемых данных. При незначительном исправлении или дополнении в вирусных базах или модулях программы применяются файлы-патчи, что сокращает объем передаваемых данных в десятки раз.

Служба вирусного мониторинга

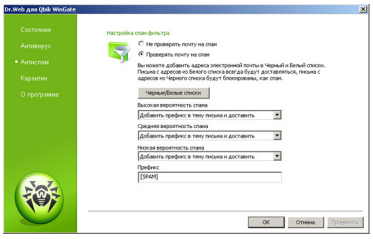
- Служба вирусного мониторинга компании «Доктор Веб» собирает по всему миру образцы вредоносных объектов, изготавливает к ним противоядия и выпускает «горячие» обновления по мере анализа новой угрозы — до нескольких раз в час.
- С момента выпуска такие обновления сразу становятся доступными для всех пользователей Dr.Web с нескольких серверов обновления в разных точках земного шара.

- С целью избежать ложных срабатываний обновления перед выпуском тестируются на огромном массиве чистых файлов.
- Интеллектуальная система автоматизированного добавления родственных вирусов позволяет максимально оперативно нейтрализовать вирусные атаки.

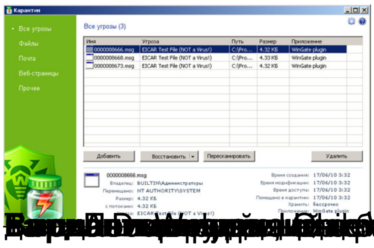
Антивирус



Антиспам



Карантин


Карантин
Все угрозы
Файлы
Почта
Веб-страницы
Прочее
Все угрозы (3)
Имя
Угроза
Путь
Размер
Приложение
0000008666.msg EICAR Test File (NOT a Virus!) C:\Pro... 4.32 КБ WinGate plugin
0000008668.msg EICAR Test File (NOT a Virus!) C:\Pro... 4.33 КБ WinGate plugin
0000008673.msg EICAR Test File (NOT a Virus!) C:\Pro... 4.32 КБ WinGate plugin
Добавить
Восстановить
Пересканировать
Удалить
0000008666.msg
Владелец: BUILTIN\Администраторы
Перемещено: NT AUTHORITY\SYSTEM
Размер: 4.32 КБ
с потоками: 4.32 КБ
Время создания: 17/06/10 3:32
Время модификации: 17/06/10 3:32
Время доступа: 17/06/10 3:32
Помещено в карантин: 17/06/10 3:32
Хранить: бессрочно

[illegible]