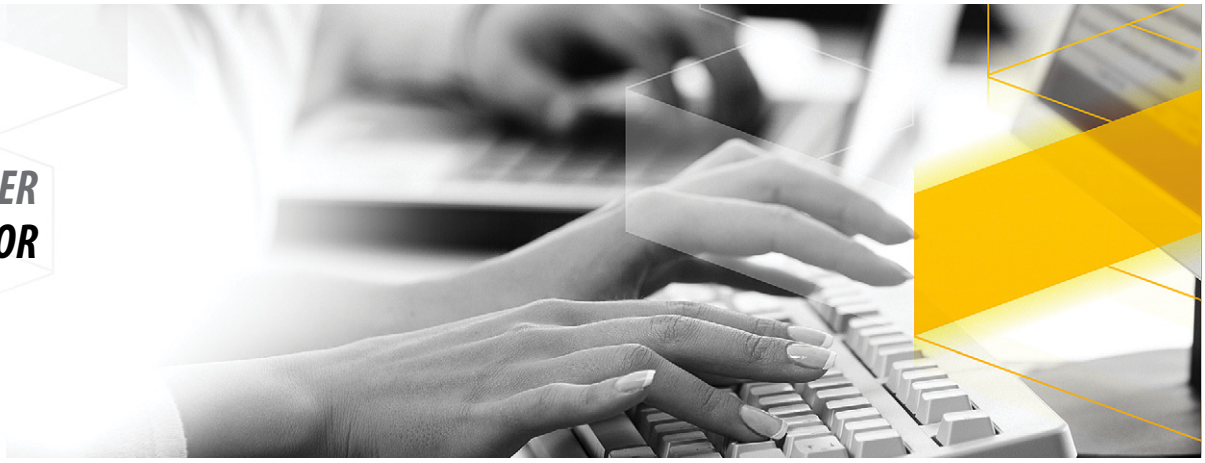
BITDEFENDER SECURITY FOR EXCHANGE



ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СЕРВЕРОВ НА ОСНОВЕ EXCHANGE

Microsoft® Exchange представляет собой критически важную службу обмена данными, которая требует защиты в целях обеспечения бесперебойной работы предприятия. Если работа сервера на основе Exchange прерывается, останавливается и работа всего персонала. Утрата работоспособности одновременно с массовым заражением вирусом, распространяемым через электронную почту, может практически парализовать предприятие. Многие организации, безусловно, осознают негативные последствия воздействия вирусов, распространяемых по электронной почте, для локальной сети предприятия, но еще более серьезным поводом для беспокойства является ущерб для репутации и вред, причиненный случайной отправкой кем-либо из сотрудников сообщения электронной почты, содержащего вирус, в адрес партнера или клиента — ведь именно потеря репутации предприятия, как ничто другое, может оказаться невосполнимой утратой.

ПОТРЕБНОСТЬ В ЗАЩИТЕ ПОЧТОВЫХ ЯЩИКОВ ОТ СПАМА

Система электронной почты предприятия является одной из главных точек корпоративной сети, через которые происходят распространение вредоносного кода и утечка данных. Таким образом, средства защиты электронной почты должны противодействовать различным угрозам, использующим электронную почту предприятия для проникновения и распространения, включая следующие:

- Отправка и получение вредоносного кода через вложения электронной почты
- Незапрашиваемая корреспонденция в форме спама
- Фишинг используется для получения доступа к конфиденциальной информации
- Утечка конфиденциальной информации через электронную почту легитимных пользователей

Ввиду того, что механизмы, используемые для распространения вирусов по электронной почте, становятся все более опасными, нейтрализовать вирус, когда он уже попал в компьютер, может быть слишком поздно. Именно поэтому развертывание решения на периферии сети и непосредственно на почтовом сервере может минимизировать воздействие вредоносного ПО путем очистки инфицированных документов и защиты коммуникаций — важнейшего ресурса предприятия.

ЗАЩИТА СЕРВЕРОВ EXCHANGE С ПОМОЩЬЮ РЕШЕНИЙ BITDEFENDER

BitDefender Security for Exchange обеспечивает защиту критически важных служб сообщений организации от вирусов, шпионского ПО и спама, распространяемых по электронной почте. BitDefender Security for Exchange предоставляет комплексную защиту от вредоносного ПО в сочетании с функциями фильтрации спама, фишинга и содержимого, что позволяет повысить производительность и обеспечить целостность платформ электронной почты в целом. BitDefender Security for Exchange выполняет сканирование сообщений электронной почты на нескольких уровнях — сначала система определяет, является ли почтовый сервер отправителя подозрительным или заблокированным, а затем проверяет наличие вредоносного кода в содержимом и вложениях или их соответствие правилам определения спама.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ПРЕИМУЩЕСТВА

- ***Сканирование входящего трафика электронной почты для обеспечения защиты от вредоносного ПО в режиме реального времени и снижения риска распространения вирусов по внутренней локальной сети***
- ***Сканирование исходящих сообщений электронной почты служит для предотвращения отправки вирусов в адрес партнеров и клиентов***
- ***Однократное сканирование всех сообщений электронной почты с использованием выбранного метода сканирования в целях снижения нагрузки на сервер***
- ***Фильтрация содержимого входящих и исходящих сообщений электронной почты, направленная на распознавание определенных администратором ключевых слов (например, данных кредитной карты)***
- ***Высокоточные спам-фильтры и фильтры фишинга на основе технологии эвристического распознавания и анализа NeuNet***
- ***Снижение стоимости ресурсов и уменьшение накладных расходов позволяет повысить общую производительность предприятия***
- ***Минимизация времени простоя сети в целях повышения эффективности эксплуатации***

Bitdefender

ВСЕСТОРОННЯЯ ЗАЩИТА

BitDefender Security for Exchange представляет собой лишь один из компонентов комплексной системы решений, полностью обеспечивающих защиту сети от шлюза до рабочей станции. Проактивные многоплатформенные решения BitDefender выполняют обнаружение и предотвращают проникновение вирусов, шпионских и рекламных программ, а также "троянских коней", способных скомпрометировать целостность сети.

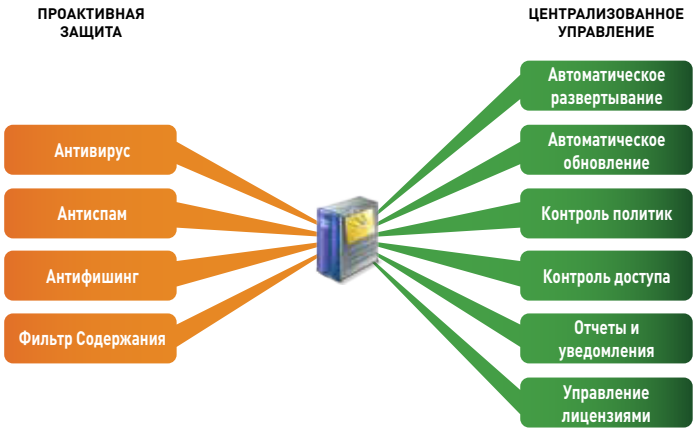
ТЕХНОЛОГИИ BITDEFENDER

b-have ***Все решения BitDefender используют патентованную технологию B-HAVE, с помощью которой выполняется анализ поведения возможного вредоносного кода в пределах виртуального компьютера, благодаря чему исключаются ложные обнаружения и значительно повышается уровень распознавания новых и неизвестных вредоносных программ.***

NeuNet ***В целях более качественного реагирования на появление новых методик рассылки спама лаборатория BitDefener разработала технологию NeuNet — мощный инструмент для фильтрации спама. В ходе апробации технологии NeuNet в лабораторных условиях была использована серия спам-сообщений, поэтому система способна обучаться распознаванию новых видов спама, анализируя сходство с обработанными ранее спам-сообщениями.***

СИСТЕМНЫЕ ТРЕБОВАНИЯ

- Windows Server 2000 SP4 с накопительным пакетом обновлений 1
- Windows Server 2003 SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server (SBS) 2008
- Windows Exchange Server 2000 SP3, 2003, 2007
- Internet Explorer 6.0 или более поздней версии



BitDefender Security for Mail Servers обеспечивает профилактическую защиту почтовых служб и централизованное управление ими

УСОВЕРШЕНСТВОВАННОЕ ПРОФИЛАКТИЧЕСКОЕ ОБНАРУЖЕНИЕ И ЗАЩИТА

Системы сканирования BitDefender признаны ведущими органами сертификации, включая ICSA Labs, Virus Bulletin и West Coast Labs, благодаря не имеющей аналогов профилактической защите от вредоносного ПО. Решения BitDefender обеспечивают расширенную защиту на нескольких уровнях.

Защита от вирусов — помимо распознавания на основе сигнатур, продукты BitDefender предоставляют технологию эвристического распознавания и анализа, при использовании которой создается эмуляция виртуального "компьютера в компьютере", после чего все файлы и код проверяются на предмет вредоносного поведения. Данная технология обеспечивает более низкий коэффициент ложно-положительного обнаружения и значительно более высокий уровень распознавания для новых и неизвестных угроз.

Защита от спама — используются постоянно обновляемые списки разрешенных сайтов и блокируемых известных спам-сайтов. Байесова самообучающаяся система обеспечивает дополнительный уровень защиты, который способен адаптироваться в соответствии с изменениями, вносимыми злоумышленниками с целью обхода статических спам-фильтров.

Защита от шпионских программ — BitDefender Security for Exchange распознает известные шпионские и рекламные программы и нейтрализует их, применяя пять способов защиты. Эти способы — отслеживание изменений реестра, сканирование файлов, управление файлами cookie, фильтрация URL-адресов и проверка содержимого — призваны предотвратить хищение важной информации.

Защита от фишинга — фишинг скорее относится к персональным угрозам, нежели к корпоративным, но при этом фишинговые сайты могут заниматься сбором персональных данных сотрудников предприятия. Используя постоянно обновляемые списки разрешенных и заблокированных сайтов, BitDefender позволяет пользователям своевременно избегать посещения известных фишинговых сайтов и, таким образом, предотвратить компрометацию данных.

Фильтрация содержимого — фильтрация содержимого позволяет распознавать предварительно определенные данные (например, данные кредитной карты или счета, наименования отчетов, базы данных клиентов и пр.) и предотвращать выход таких данных из-под контроля предприятия.

Список разрешенных и заблокированных серверов служит для исключения отдельных почтовых серверов или назначения определенных почтовых серверов в качестве доверенных с функцией проверки их IP-адресов для сопоставления с доменом отправителя.

МНОГОЧИСЛЕННЫЕ ПОЛНОСТЬЮ НАСТРАИВАЕМЫЕ МЕТОДЫ СКАНИРОВАНИЯ

BitDefender Security for Mail Servers предоставляет следующие технологии сканирования: непрерывное, по запросу, полное и транспортное сакнирование. Это позволяет распознавать вредоносный код в целях защиты целостности служб электронной почты. Каждый из указанных методов сканирования применяется только один раз для сканирования всех сообщений электронной почты. При этом в каждое сканированное сообщение может быть добавлен полностью настраиваемый нижний колонтитул. Также можно настраивать дополнительные методы сканирования содержимого во избежание рассылки выбранными группами пользователей конфиденциальной информации.

ИНТЕГРАЦИЯ С ПЛАТФОРМОЙ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ BITDEFENDER

Решение BitDefender for Mail Servers позволяет осуществить интеграцию с контрольной панелью безопасности сервера управления, благодаря чему для администраторов обеспечивается визуальный доступ к сетевым ресурсам и комплексным средствам обеспечения безопасности в масштабах предприятия. Сервер управления BitDefender Management Server предоставляет централизованную точку для удаленной установки, настройки и отчетности по всем продуктам BitDefender Clients, Server и Gateway, развертываемых в рамках предприятия; а также оповещает администраторов о выполнении сканирования, обнаружении инфицированных файлах и задачах обновления посредством многоцелевого модуля оповещения.

Bitdefender