

Как защитить почтовый сервис от вредоносных программ без увеличения выделяемых ресурсов

Электронная почта – это **главная точка входа вредоносного ПО** в компаниях, угрожающего корпоративному имиджу, ведь при проникновении инфекции существует риск инфицирования клиентов, партнеров и провайдера организации. Во избежание этого, в каждом сетевом компоненте должна быть внедрена стратегия послойной защиты для борьбы со шпионами, вирусами и червями, фишингом и другими Интернет-угрозами, которые пытаются проникнуть в SMTP-сервер.

С другой стороны, пытаясь сохранить пространство для хранения информации, а также Интернет-канал с помощью фильтрации вирусов и нежелательной почты, тем не менее, не следует усложнять администрирование защиты или заметно увеличивать время отклика системы.

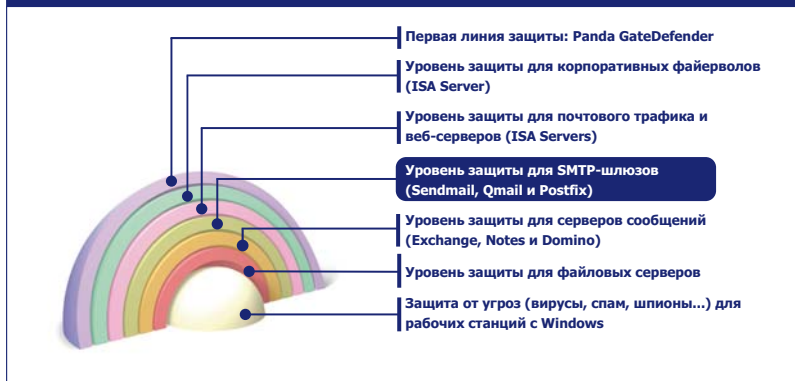
Легко используемое и настраиваемое решение для защиты от вредоносного ПО, позволяющее получить максимум от ресурсов сервера

Panda Security for Qmail предоставляет в режиме реального времени эффективную защиту всего SMTP-трафика Вашей компании на серверах и шлюзах Qmail, предотвращая повышенное использование IT-ресурсов и проникновение в корпоративную сеть вирусов и вредоносных программ.

Благодаря усовершенствованному эвристическому движку, **Panda Security for Qmail** автоматически обнаруживает и блокирует спам. В результате, снижается нагрузка на Интернет-канал и уменьшаются необоснованные затраты рабочего времени сотрудников. Гибкие опции настройки продукта позволяют Вам быстро и легко включить или исключить домены и адреса электронной почты в процессе сканирования.

Стратегия многоуровневой защиты

Panda for Qmail предоставляет защиту периметра SMTP-шлюза.



Основные выгоды

- Настраиваемые политики безопасности помогают защитить **корпоративный имидж**, исключить ситуации несоблюдения правил, предотвратить промышленный шпионаж, кражу регистрационных данных и т.д.
- **Увеличивает** производительность администратора и конечного пользователя.
- **Максимизирует безопасность почтовых коммуникаций**, предотвращая их распространение.

Ключевые характеристики

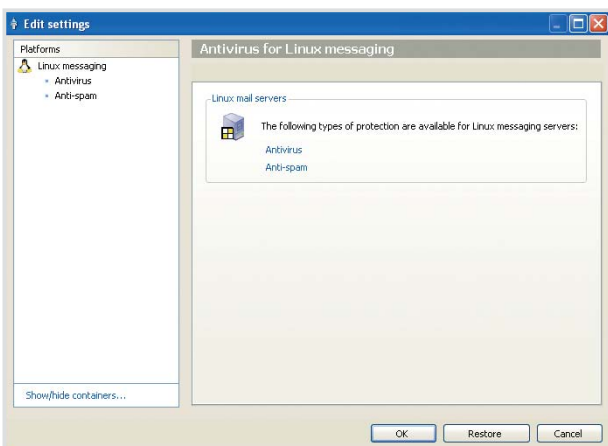
- **Сканирование и лечение в режиме реального времени** всего входящего и исходящего корпоративного SMTP-трафика.
- **Полная и тщательная защита от спама** – легко настраивать и устанавливать.
- **Обнаружение и блокировка всех типов вредоносных программ**: вирусы, черви, троянцы, шпионы, фишинг, дозвонщики, риски безопасности...
- **Гибкая настройка** защиты и почтовых доменов и аккаунтов для инспектирования. Также предоставляет настраиваемые предупреждения и оповещения.
- **Централизованное и удаленное администрирование** через веб-консоль и консоль AdminSecure для администрирования и внедрения программ под Windows.
- **Отличная интеграция** решения в защищаемый сервер Qmail.
- **Оптимизированная производительность в шлюзах Linux** благодаря своим усовершенствованным технологиям поиска вредоносных программ.

Сканирование SMTP-трафика в режиме реального времени

Panda for Qmail выгодно отличается возможностями сканирования на вирусы входящего и исходящего SMTP-трафика в режиме реального времени. Вся почтовая коммуникация полностью защищена от вредоносных программ, т.к. осуществляется сканирование сжатых вложений (на любом уровне), вложенных или встроенных документов, а также содержание (текст или HTML) всех сообщений.

Полная и тщательная защита от спама

Panda for Qmail содержит усовершенствованный антиспамовый движок, основанный на **правилах, списках, сигнатурах, Байесовых алгоритмах и удаленном обучении**, которые позволяют оптимизировать тщательность процесса классификации спама. **Panda for Qmail** обнаруживает мистификации и нежелательную почту, которые используют ложные NDR-сообщения. Содержащий различные уровни чувствительности, продукт включает отправителей и домены в белые и черные списки, и дополнительно ставит в теме сообщения пометку с идентификацией спама, чтобы наглядно показать пользователю характер данного письма, не отрывая его при этом от своей работы.



Обнаружение и блокировка угроз

Panda for Qmail постоянно проверяет почту на поиск вредоносного кода: вирусов, червей, троянцев, шпионского и рекламного ПО, фишинга, дозвончиков, рисков безопасности и т.д.

Более того, усовершенствованный движок *Genetic Heuristic Engine* (GHE) в **Panda for Qmail**, обнаруживает новые угрозы и изолирует подозрительный код. При этом продукт в течение нескольких часов автоматически запрашивает в Panda анализ кода для оперативного устранения угрозы, о чем сообщает отправителю или получателю сообщения.

Персонализированные гибкие настройки

Гибкая конфигурация в **Panda for Qmail** адаптируется к Вашим текущим потребностям, позволяя Вам конфигурировать и выбирать домены и адреса электронной почты для сканирования или исключения из сканирования, а также полностью удалять инфицированные сообщения для предотвращения перегрузки почтовых серверов от атак на отказ в обслуживании (Denial of Service, DoS).

Централизованное и удаленное управление

Panda for Qmail может управляться из двух административных консолей для облегчения процесса установки, мониторинга инцидентов и обновлений внутри сети.

В дополнение к традиционной веб-консоли управления продуктом, основанной на Apache, **Panda for Qmail** теперь предлагает и Windows-консоль управления **Panda AdminSecure**. Данный инструмент удаленного управления контролирует уровень защиты каждого почтового сервера (как и всех других решений Panda) с использованием графических отчетов, предупреждений и т.д., что позволяет предоставить в режиме реального времени глобальный взгляд на статус защиты предприятия.

Цельная интеграция с SMTP-серверами

Новые техники, используемые вредоносными программами для своего распространения, заставляют организовывать защиту периметра, которая была бы на 100% надежна и полностью совместима со всеми платформами. **Panda for Qmail** отлично интегрируется с SMTP-шлюзами Linux, блокируя частично отправленные сообщения и обнаруживая сообщения, содержащие эксплойты уязвимостей, без снижения производительности системы.

Оптимальная производительность в шлюзах Linux

В продукте применены самые современные технологии разработки ПО, благодаря чему он предоставляет **максимальную и надежную производительность** на Qmail-серверах. В частности, это стало возможным, благодаря способности продукта сканировать сжатые файлы в памяти, вместо их предварительного сохранения на диск.

Технические требования

Процессор Pentium 200 МГц, 64 МБ ОЗУ и 90 МБ свободного пространства на жестком диске. Операционная система для интеграции с AdminSecure или независимой установки: Red Hat 7.2, 9, Red Hat Enterprise 2.1, 3 AS/ES, Red Hat Enterprise 4 AS/ES, Debian 3.0, 3.1, Mandrake 9.0, 9.1, 10, Mandrake Corporate Server 4.0, Suse 8.1, 8.2, 9.0, 9.1 Professional, 9.2 Professional, Suse 9 Enterprise Server, Suse 10 Enterprise Server.

Веб-консоль: Internet Explorer 4.0 (или выше), Netscape Navigator 4.6 (или выше).

Panda AdminSecure: Pentium III 800 МГц, 512 МБ ОЗУ, 512 МБ свободного пространства на жестком диске. Операционные системы: Windows NT4 SP6, 2000, XP, Vista 32 & 64 bit, Server 2003.

"Panda Antivirus намного быстрее других антивирусов, которые мы использовали ранее. Центральное администрирование намного более эффективное."

Майкл Дэвенпорт, Continental Plastics Company, США.



Panda Security for Qmail можно приобрести отдельно или в составе **Panda Security for Enterprise**.

Посетите www.pandasecurity.com
Получите Вашу демо-версию Panda Security for Qmail.

PANDA SECURITY | **20th Anniversary**
1990-2010