

## Гибкое управление защитой от вирусов, спама и шпионов для всех пользователей

**Postfix-сервера** никогда не имеют одинаковой конфигурации, таких нет даже в одной и той же компании, т.к. они должны быть четко настроены в соответствии с теми функциями, которые они выполняют (почтовый шлюз или сервер), профилями пользователей, чьими ящиками они управляют, и характеристиками компьютеров, на которых они работают.

**Почтовый сервис, предлагаемый такими серверами, должен быть защищен** от вторжений и других угроз со стороны хакеров, которые пытаются проникнуть в сеть компании через корпоративный периметр сети, чтобы украсть информацию, активизировать свои вредоносные программы или прервать работу пользовательских сервисов.

Подобная ситуация требует применения против каждого типа вредоносного ПО **последовательной и настраиваемой политики безопасности**, которая адаптируется к потребностям каждого Postfix-сервера.

## Легко управляемое и настраиваемое решение, предлагающее полную защиту для SMTP-почты

**Panda Security for Postfix** предлагает специальную защиту от вредоносных программ для сообщений, отправляемых или принимаемых **через SMTP** в почтовых серверах Postfix, используемых компаниями и провайдерами.

provides specific anti-malware protection for messages received **via SMTP** in the Postfix mail systems used by companies and ISPs.

**Panda Security for Postfix отлично интегрируется с Postfix**, который работает в качестве независимого шлюза (трафик-канал к другим серверам) или в качестве почтового сервера (доставляя электронную почту к их конечным пунктам назначения).

### 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.
- Достигает **наибольшей полезности использования ресурсов почтового сервера** для оптимизации качества сервисов

### Ключевые характеристики

- **Полная защита для почтового трафика. Обнаруживает все вредоносные программы** (вирусы, шпионы и т.д.). Сообщение удаляется целиком в случае атаки типа "отказ в обслуживании" (DoS).
- **Полная и тщательная защита от спама** – легко настраивать и устанавливать.
- **Блокировка новых угроз** надежными эвристическими технологиями.
- **Оптимизированная производительность и диапазон обнаружений**, основанные на сканировании в памяти.
- **Цельная интеграция с технологиями Postfix.**
- **Централизованное и удаленное администрирование** с помощью веб-консоли и консоли управления AdminSecure для управления и и внедрения программ под Windows.
- Автоматические **ежечасные обновления** сигнатурного файла.

### Стратегия многоуровневой защиты

**Panda for Postfix** предоставляет защиту периметра SMTP-шлюза.



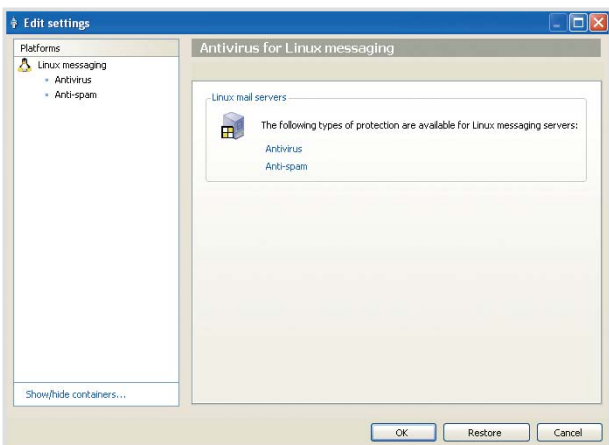
## Полная защита электронной почты

**Panda for Postfix** выгодно отличается способностью сканировать и дезинфицировать вредоносные программы в теле сообщений в любом формате: обычный текст или HTML. Продукт может также проверять вложенные файлы, сжатые файлы, вложенные сообщения, и даже встроенные OLE-объекты для защиты от всех типов вредоносных программ, таких как: шпионское и рекламное ПО, фишинг, черви, троянцы, дозвонщики, шутки, риски безопасности и хакерские утилиты.

**Panda for Postfix** сканирует все сообщения: те, что отправляются на почтовые сервера Postfix, и те, что отправляются на другие сервера, используя контент-фильтр Postfix.

## Полная и тщательная защита от спама

**Panda for Postfix** содержит улучшенный антиспамовский движок, основанный на **правилах, списках, сигнатурах, Байесовых алгоритмах и удаленном обучении** для оптимизации и тщательности процесса классификации спама. **Panda for Postfix** обнаруживает мистификации и нежелательную почту, которые используют ложные NDR-сообщения. Предлагая различные уровни чувствительности, продукт позволяет включать отправителей и домены в белые и черные списки, и идентифицирует спам в теме сообщения для дополнительного привлечения внимания пользователей.



## Блокировка новых угроз

Усовершенствованный движок *Genetic Heuristic Engine (GHE)* в **Panda for Postfix** обнаруживает новые угрозы и изолирует новый подозрительный код. Продукт также автоматически запрашивает в Panda анализ кода для оперативной дезинфекции угроз и сообщения об этом отправителю или получателю сообщения.

## Оптимизированная производительность и способность обнаружения

**Panda for Postfix** способен адаптироваться к Вашим текущим потребностям, предоставляя возможность конфигурации и выбора доменов и адресов электронной почты для сканирования или исключения из сканирования, и позволяя защите быть приоритетной задачей, если сервер становится загруженным.

Инновационная технология продукта сканирует все типы сжатых файлов в памяти значительно быстрее, чем если бы они были предварительно скопированы на жесткий диск. В результате этого продукт обладает оптимальной производительностью сканирования и более быстрой обработкой сообщений.

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

## Максимальная интеграция с Postfix

В дополнение к сканирующему движку последнего поколения, **Panda for Postfix** использует современные технологии, рекомендованные для интеграции с Postfix и дистрибутивами Linux. Продукт работает с максимальной производительностью в мультипоточковых окружениях с несколькими процессорами. В результате, продукт является идеальным решением для подобных платформ.

## Удаленное централизованное управление

**Panda for Postfix** может управляться с помощью любой из двух консолей управления, облегчая процессы установки, мониторинга инцидентов и обновлений внутри сети.

В дополнение к традиционной веб-консоли управления продуктом, **Panda for Postfix** 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.

## Автоматические ежедневные обновления

Обновления **Panda for Postfix** могут быть настроены в автоматическом режиме без какого-либо вмешательства со стороны пользователя каждый час. Инкрементные обновления сигнатурного файла помогают снизить потребление Интернет-канала и сгладить пики коммуникационного трафика.

## 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 или 9, Red Hat Enterprise 2.1, 3 AS/ES или 4 AS/ES, Debian 3.0 или 3.1, Mandrake 9.0, 9.1 или 10, Mandrake Corporate Server 4.0, Suse 8.1, 8.2, 9.0, 9.1 Professional, 9.2 Professional, 9 Enterprise Server или 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.



Посетите [www.pandasecurity.com](http://www.pandasecurity.com)

Получите Вашу демо-версию Panda Security for Postfix.

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