Dr.WEB®
с 1992

Защити созданное

Сравнения решений для защиты почты на основе операционных систем типа Unix

125124, Россия, Москва,
3-я улица Ямского поля,
вл. 2, корп. 12а

Телефон:
+7 (495) 789-45-87

Факс:
+7 (495) 789-45-97

www.drweb.com
www.av-desk.com
www.freedrweb.com
www.drweb-curenet.com

Dr.WEB®
с 1992

В данном сравнении рассматриваются решения компаний «Доктор Веб», «Лаборатория Касперского» и Eset. В обзоре использовались как интегрирующиеся в почтовые серверы решения, так и устанавливающиеся отдельно – в виде SMTP-сервиса.

Продукты, участвующие в сравнении:

Dr.Web для почтовых серверов Unix, Dr.Web для почтовых шлюзов Unix 5.01	Kaspersky Security for Mail Server 5.6*	Eset Mail Security

* Продукт включает в себя следующие компоненты:

- Kaspersky Administration Kit
- Антивирус Касперского для Microsoft Exchange (Antivirus Corporate Suite для MS Exchange)
- Антивирус Касперского для Lotus Notes/Domino
- Антивирус Касперского для Linux Mail Server
- Kaspersky Security Mail Gateway

Купив продукт, пользователь имеет право устанавливать любой из его компонентов.

Таблица функционала

Функционал	Kaspersky Linux Mail Server/ Mail Gateway 5.6	NOD32 Linux Mail Server	Dr.Web 5.01
Возможность установки в качестве Proxy	✓		✓
Возможность интеграции в почтовые системы	✓	✓	✓
Наличие в продукте антивирусного сканера	✓		✓
Антиспам-проверка трафика	✗	✓	✓
Антивирусная проверка трафика	✓	✓	✓
Управление системой через веб-интерфейс, включая доступ к личным карантинным папкам			✓
Мониторинг системных ресурсов	✓		✓
Управление рабочей очередью приложения (просмотр, отправка, удаление)/ограничение количества одновременно проверяемых объектов			✓
Работа с несколькими почтовыми системами с различными настройками			✓
Управление производительностью решения			✓
Удобство контроля состояния сети			

Наличие в продукте агента удаленной системы управления и настройки	Через Webmin		Через Webmin
Функции установки и обновления			
Возможность обновлений по требованию	✓		✓
Возможность автоматических обновлений	✓		✓
Возможность настройки расписания обновлений	✓		✓
Возможность указания альтернативных источников обновлений	✓		✓
Возможность получения обновлений из Интернет/локальной сети	✓		✓
Возможность добавления своих модулей/ интеграции в чужие решения	✗		✓
Проверка настроек	✓		✓
Импорт настроек предыдущих версий	✓		✓
Откат настроек			✓
Контроль корректности функционирования модулей специальным процессом	✓		✓
Гибкость при выборе политик информационной безопасности			
Многоуровневая система определения спама (спам / возможно, спам)	✓		✓
Отсутствие необходимости обучения антиспама, в том числе через клиентов у пользователей	✗		✓
Проверка имен доменов и IP-адресов отправителей по черным и белым спискам	✓	✓	✓
Проверка доменного имени отправителя	✓		✓
Возможность настройки параметров сканирования для каждого почтового ящика			✓
Возможность помещать письма в карантинную зону	✓		✓
Запрос на указанный адрес отправителя (блокировка в случае отсутствия ответа)			✓
Ограничение максимального количества пересылок	✓		✓
Ограничение по максимальному размеру письма	✓		✓

Ограничение по максимальному размеру писем, принятых за одну сессию			✓
Ограничение по максимальному количеству писем с одного адреса	✓		✓
Проверка заголовков на соответствие спецификации RFC-822			✓
Анализ заголовков и тела по формальным признакам	✓		✓

Авторизация пользователя с помощью имени и пароля, IP–адреса

			✓
Фильтрация элементов сообщений по ключевым словам, фразам или шаблонам	✓		✓
Фильтрация данных по объему и типам вложений	✓		
Архивирование и регистрация сообщений	✓		✓
Использование внешних баз данных	✓		✓
Удаленное хранение архивов	✓		✓
Возможность помечать и модифицировать письма	✓	✓	✓
Возможность пересылать на определенный адрес или адреса	✓		✓
Возможность реализации нескольких действий	✓		✓
Использование правил обработки сообщений, в том числе задание правил для отдельных пользователей			✓
Ограничение времени проверки сообщения			✓
Обработка сообщений на спам-ловушки			✓
Возможность маршрутизации сообщений			✓
Определение типов файлов по сигнатуре	✓		✓
Обработка сжатых/архивных файлов	✓		✓
Блокирование программ-закладок, вредоносного мобильного кода и т.д.	✓		✓
Формирование отчетов и статистики			

Накопление статистики о работе системы	✓		✓
Генерация отчетов	✓		✓
Возможность настройки отчетов	✓		✓
Оповещение администраторов и пользователей об угрозах различного типа			
Отсылка уведомлений администратору	✓		✓
Использование шаблонов уведомлений	✓		✓
Использование управляющих писем			✓

Выводы

Все решения для защиты почты являются высокоинтеллектуальными системами, предназначенными для работы с большими потоками сообщений. Более того, лидеры отрасли во многом похожи по списочному функционалу. В связи с этим при их приобретении важно обращать внимание на:

- возможность гибкой настройки под потребности пользователей;
- возможность использования решения в условиях отсутствия высококвалифицированных специалистов;
- системные требования решения;
- удобные условия лицензирования.

Возможность гибкой настройки под потребности пользователей

В отличие от продукта «Лаборатории Касперского», настраиваемого через статические параметры конфигурационного файла, решение от «Доктор Веб» может настраиваться через правила, что значительно повышает гибкость решения - клиент практически не ограничен при реализации своих требований информационной безопасности, что особенно важно в условиях вступления в силу закона о защите персональных данных.

Возможность использования решения в условиях отсутствия высококвалифицированных специалистов

Несмотря на богатство возможностей, решение от «Доктор Веб» не требует длительной настройки перед введением в строй. Кроме того, необходимо сказать, что это решение может поставляться не только в виде программного продукта, но и в составе программно-аппаратного комплекса - сервера, спроектированного для работы по принципу «поставил и забыл».

Системные требования решения

Решения от «Доктор Веб» традиционно отличаются низкими системными требованиями, что особенно актуально для тех компаний и организаций, которые не имеют возможности постоянно обновлять свои серверы под растущие системные требования большинства антивирусных продуктов.

Dr.WEB®
с 1992

Удобные условия лицензирования

Продукты компании «Доктор Веб» лицензируются более удобным для пользователя способом: клиент покупает только тот продукт, который ему нужен, и не переплачивает за «избыточный» функционал. Покупая решение от «Лаборатории Касперского», клиент получает решения для всех поддерживаемых систем (Exchange, Lotus...), даже если они ему не нужны. Что, естественно, сказывается на стоимости.

Также преимуществами решений компании «Доктор Веб» перед решением от «Лаборатории Касперского» являются:

- Наличие возможности фильтрации на спам. Решение для фильтрации спама от «Лаборатории Касперского» поставляется в виде отдельного продукта и не всегда может быть установлено на одном сервере с продуктом для фильтрации вирусов, что не только усложняет установку и сопровождение получившегося комплекса, но и сказывается на его стоимости.
- Возможность как интеграции самого продукта в решения других производителей, так и добавления нового функционала через открытое API.
- Возможность реализации правил обработки сообщений, в том числе задание правил для отдельных пользователей.
- Возможность обработки сообщений через управляющие письма.
- Возможность работы с несколькими почтовыми системами с различными настройками.

Решение от компании Eset лучшим образом характеризует то, что для своей работы оно использует свободно распространяемый скрипт AMaViS (которое может использовать для сканирования сообщений и ядро от компании «Доктор Веб»!). То есть оно является лишь интерфейсом к бесплатному решению. Список возможностей продукта можно оценить по размеру документации – в ней всего 24 страницы, причем лишь около пяти из них посвящены настройке системы. Остальные описывают установку, обновление и схему работы приложения. Для сравнения, документация для системного администратора по продукту Dr.Web для почтовых серверов Unix насчитывает 188 страниц.