kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Security для почтовых серверов

Проверенная защита нового поколения для корпоративной почты

Электронная почта – основной канал, по которому в корпоративные системы проникает вредоносное ПО[1]. Решение Kaspersky Security для почтовых серверов защищает электронную почту от программ-шифровальщиков, вредоносных вложений, спама, фишинга и неизвестных угроз, используя современную эвристику, песочницы, машинное обучение и другие передовые технологии.

Надежные и широко признанные средства защиты помогут вашей компании избежать финансового, операционного и репутационного ущерба, вызванного атаками через электронную почту.

Основные возможности

- Защита от вредоносного ПО в режиме реального времени или по запросу
- Двусторонняя интеграция с Kaspersky Anti Targeted Attack Platform (KATA)
- Управление корпоративной электронной почтой с проверкой подлинности помогает бороться с ее компрометацией
- Защита от угроз «нулевого дня»
- Доступ к глобальным аналитическим данным об угрозах в сети Kaspersky Security Network
- Поддержка LDAP/ Microsoft Active Directory
- Управление карантином для электронных писем и вложений
- Защита от внедренных вредоносных макросов и других объектов
- Остановка распространения по электронной почте программ-шифровальщиков

Преимущества

Зашита от спама и повышение производительности

Kaspersky Security для почтовых серверов – это решение нового поколения, которое обнаруживает даже самый сложный неизвестный спам. Благодаря минимальному уровню ложных срабатываний, оно делает работу сотрудников с электронной почтой комфортной – в их почтовых ящиках только деловая переписка, без спама и фишинговых сообщений.

Защита от фишинга с помощью нейросетей

Предлагаемая «Лабораторией Касперского» передовая защита от фишинга опирается на нейросетевой анализ для повышения эффективности обнаружения. Эта облачная технология использует более 1000 критериев, включая анализ изображений, языковые проверки и сигнатуры скриптов, и опирается на собираемые со всего мира данные о вредоносных и фишинговых URL-адресах, чтобы защищать пользователя как от известных, так и от неизвестных фишинговых электронных писем и угроз «нулевого дня».

Снижение стоимости владения

Kaspersky Security для почтовых серверов предлагает сбалансированное сочетание управляемости и простоты использования, высвобождая время IT-специалистов для других задач. Гибкие сценарии настройки фильтрации позволяют оптимально адаптировать решение к существующим бизнес-процессам и сократить потребность в ресурсах для управления.

1 Отчет Verizon о расследованиях нарушений безопасности данных (Verizon Data Breach Investigations Report), 2017.

Функции

HuMachine™ – многоуровневая защита от вредоносного ПО

Созданное «Лабораторией Касперского» новое поколение защитных решений включает несколько уровней проактивной защиты и использует машинное обучение и облачную аналитику угроз для выявления во входящей почте вредоносных вложений и программ, как известных, так и новых. Доступна проверка в режиме реального времени и по запросу – последняя особенно полезна в сценариях миграции.

Глобальная аналитика угроз
Kaspersky Security для почтовых серверов составляет актуальную картину угроз на основе данных, собираемых со всего мира, обновляя ее по мере изменения.

Машинное обучение
Глобальная аналитика угроз с использованием больших данных опирается на сочетание мощных алгоритмов машинного обучения с опытом экспертов. В результате высокий уровень обнаружения сочетается с минимальным числом ложных срабатываний.

Эмуляция в песочнице
Для защиты от самого сложного, тщательно замаскированного вредоносного ПО вложения запускаются и анализируются в безопасной среде.

Управление email-аутентификацией

Надежные механизмы аутентификации электронной переписки, такие как SPF, DKIM и DMARC, помогают обеспечить защиту от атак через поддельные домены.

Фильтрация вложений

Некоторые типы вложений слишком опасны. Решение «Лаборатории Касперского» позволяет гибко настроить политику доставки для фильтрации вложений и распознает множество типов маскировки файлов, которые часто используются киберпреступниками. Эти функции помогают снизить вероятность утечки данных.

Встроенное резервное копирование

Чтобы гарантировать защиту от потери критически важных данных при лечении или удалении зараженных данных, исходные сообщения можно сохранять в резервном хранилище, где администратор может обработать их в любое удобное время. Для условного резервного копирования данных можно настроить специальные правила.

Интеграция с платформой Kaspersky Anti Targeted Attack Platform

Двусторонняя интеграция с решением «Лаборатории Касперского» для защиты от целевых атак позволяет не только использовать почтовые системы как дополнительный источник информации для обнаружения целенаправленных атак, но также блокировать дальнейшее распространение сообщений с опасным содержимым в зависимости от результатов глубокого анализа Kaspersky Anti Targeted Attack Platform.

www.kaspersky.ru

Приложения в составе продукта

- **Kaspersky Security для Linux Mail Server**
- **Kaspersky Security для Microsoft Exchange Server**
- **Kaspersky Secure Mail Gateway**
- **Kaspersky Security Center**

Как приобрести

Kaspersky Security для почтовых серверов продается отдельно, а также является частью решения Kaspersky Total Security для бизнеса.