kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Security для почтовых серверов

Надежная защита электронных коммуникаций

Электронная почта – основной канал, по которому в корпоративные системы проникает вредоносное ПО, угрожающее IT-безопасности бизнеса. Злоумышленники используют все более изощренные способы атаки через электронную почту. В результате компании несут финансовые, производственные и репутационные потери. Чтобы избежать этого, организациям необходимо повышать уровень защиты и устойчивость к киберугрозам. Укрепив инфраструктуру и сократив поверхность атаки, вы сделаете свой бизнес менее привлекательной или вовсе недосягаемой целью для злоумышленников. Лучше принять меры, чтобы предотвратить попадание нежелательных писем и вредоносного ПО на рабочие места пользователей корпоративной сети.

В 2019 году мы заблокировали **почти полмиллиарда попыток фишинговых атак**

Securelist, отчет о спаме и фишинге за 2019 год

Фильтрация подозрительной и нежелательной почты на уровне шлюза

Большинство email-атак срабатывают только на рабочей станции – Kaspersky Security для почтовых серверов позволяет остановить их еще на этапе попадания в корпоративную сеть через шлюз. Это проверенное временем решение обеспечит устойчивость вашей инфраструктуры, обнаруживая и перехватывая атаки на раннем этапе, до того, как они распространятся по системе и поставят ваш бизнес под угрозу – независимо от наличия и уровня защиты конечных устройств.

Быстрая и точная обработка безопасных писем

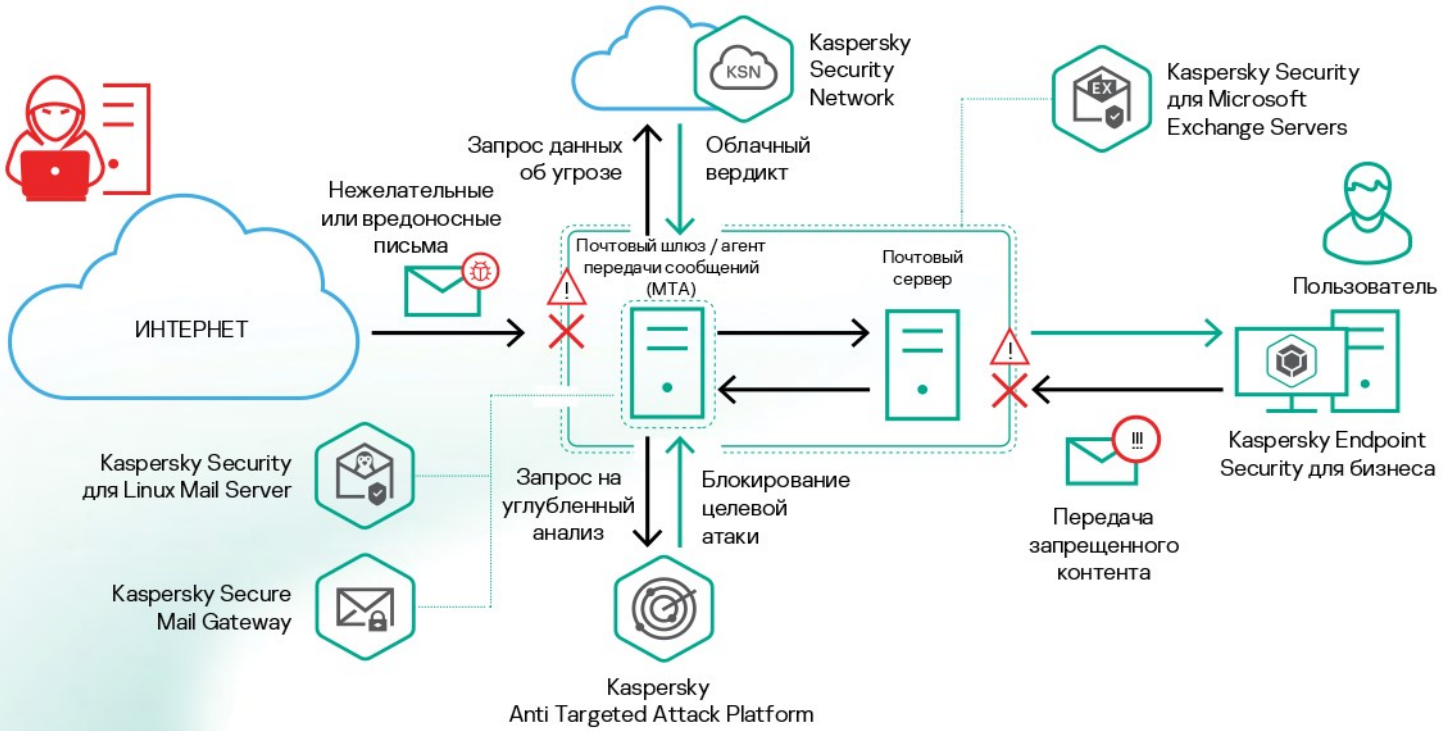
Электронная почта играет ключевую роль в бизнес-коммуникациях. А значит, защита электронной почты должна работать эффективно и не мешать корпоративным коммуникациям. Kaspersky Security для почтовых серверов предлагает наиболее эффективную[1] защиту от всех видов киберугроз: от массового фишинга и спама до компрометации корпоративной электронной почты (BEC) и программ-вымогателей – без препятствий для обмена безопасными сообщениями и практически без ложных срабатываний.

Защита электронной почты не только на уровне шлюза

Помимо защиты серверов, необходимо защищать и самих корпоративных пользователей – в том числе и от самих себя, а ваш бизнес – от ошибок ваших сотрудников. Kaspersky Security для почтовых серверов уже на уровне отдельных учетных записей на серверах Microsoft Exchange может выявлять вредоносный или нежелательный контент – в том числе вредоносное ПО, фишинговые письма и потенциально опасные вложения – в соответствии с политиками, настраиваемыми администратором. Мы настоятельно рекомендуем настроить защиту на уровне почтовых ящиков, чтобы не допустить перехвата учетных данных или распространения внутренних угроз.

1 http://www.kaspersky.ru/top3

Основные возможности



Модель атаки через электронную почту

Многоуровневая защита от вредоносного ПО

Многоуровневая защита на основе самообучающихся нейросетей предотвращает даже самые изощренные атаки через электронную почту, в том числе атаки с использованием исполняемых файлов, встроенных объектов и вредоносных скриптов. Поведенческий анализ, облачные данные о репутации, сигнатурные модули, эвристические и сигнатурные базы данных в сочетании со знаниями экспертов обеспечивают эффективное многоуровневое обнаружение и предотвращение угроз с минимальным количеством ложноположительных срабатываний.

Песочница

Для защиты от самого сложного и тщательно замаскированного вредоносного ПО вложения запускаются и анализируются в безопасной среде (песочнице). Поэтому опасные экземпляры не попадают в корпоративную систему. Интеграция с платформой Kaspersky Anti Targeted Attack позволяет выполнять подозрительный код во внешней песочнице для более глубокой оценки и динамического анализа. Целевую атаку можно прервать, заблокировав доставку компонентов.

Автоматическая защита от спама (на основе репутации содержимого и адреса отправителя)

Интеллектуальные компоненты защиты от спама минимизируют число ложных срабатываний и адаптатируются к изменениям в ландшафте угроз, блокируя поток нежелательных писем. Репутационные данные из источников по всему миру обрабатываются в облаке, формируя базу для надежного отслеживания спама.

Защита от компрометации корпоративной электронной почты

Специальная система обнаружения угроз на основе машинного обучения, алгоритмические модели которой постоянно дополняются новыми сценариями, обрабатывает косвенные индикаторы угроз. Это позволяет блокировать мошеннические письма, даже если они убедительно составлены и отправлены с легитимных адресов. Поддержка таких механизмов аутентификации отправителя, как SPF, DKIM и DMARC, защищает от спуфинга.

Защита на уровне почтового ящика

Решение защищает не только на уровне шлюза, но и на уровне почтовых ящиков. Для этого используются следующие технологии:

- Повторная проверка электронных писем для защиты от отложенной активации фишинговых URL-адресов
- Временный карантин для защиты от спама подходит для сред с жесткими требованиями к безопасности. В неоднозначных случаях подозрительные письма можно поместить на временный карантин, пока Kaspersky Security Network не соберет достаточно данных, чтобы определить, безопасны ли они.

Улучшенная защита от фишинга

Наша технология защиты от фишинга основана на нейросетевом анализе. Она задействует более 1000 критериев, включая анализ изображений, языковые проверки и специфические скрипты, и опирается на собираемые со всего мира данные о вредоносных и фишинговых URL- и IP-адресах для защиты от известных и неизвестных фишинговых угроз и угроз «нулевого часа».

Предотвращение небезопасной передачи контента

Система настраиваемой контентной фильтрации выявляет методы маскировки файлов, которые часто используют злоумышленники, и определяет потенциально опасные вложения, чтобы предотвратить их передачу. Администраторы могут гибко конфигурировать политики безопасности, предотвращающие утечку данных.

Встроенное резервное копирование

Чтобы предотвратить потерю критически важной информации при лечении или удалении зараженных данных, можно сохранять резервные копии исходных сообщений – администратор сможет их обработать в любое удобное время. Предусмотрена возможность настройки специальных правил резервного копирования.

Управление и прозрачносwть

Простой и наглядный веб-интерфейс позволяет администратору управлять защитой и отслеживать ее статус благодаря инструментам:

- гибкого конфигурирования правил и политик
- интеграции с Active Directory
- экспорта событий в SIEM-систему
- диагностики состояния системы

Как приобрести

Kaspersky Security для почтовых серверов можно приобрести в качестве отдельного решения или в составе Kaspersky Total Security для бизнеса и Kaspersky Total Security Plus для бизнеса.

Состав продукта

- Kaspersky Security для Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security для Microsoft Exchange Servers

www.kaspersky.ru