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.

Основной канал утечки данных

- Согласно отчету Verizon, социальная инженерия – самый популярный тип атаки, приводящий к утечкам данных.
- Авторы отчета отмечают, что в течение последних двух лет фишинг оставался одной из самых распространенных угроз.

Источник: **отчет Verizon о расследованиях нарушений безопасности данных (Verizon Data Breach Investigations Report)**

Защита основной точки входа для атак

Kaspersky Security для почтовых серверов повышает устойчивость к атакам через электронную почту.

Фильтрация подозрительной и нежелательной почты на уровне шлюза

Большинство атак через электронную почту приводятся в действие только на рабочих местах. Kaspersky Security для почтовых серверов останавливает их еще на этапе попадания в корпоративную сеть через шлюз. Это проверенное временем решение обеспечит устойчивость вашей инфраструктуры, обнаруживая и перехватывая атаки в самом начале цепочки поражения – прежде чем они проникнут внутрь периметра и атакуют пользователей и конечные устройства.

Быстрая и точная обработка безопасных писем

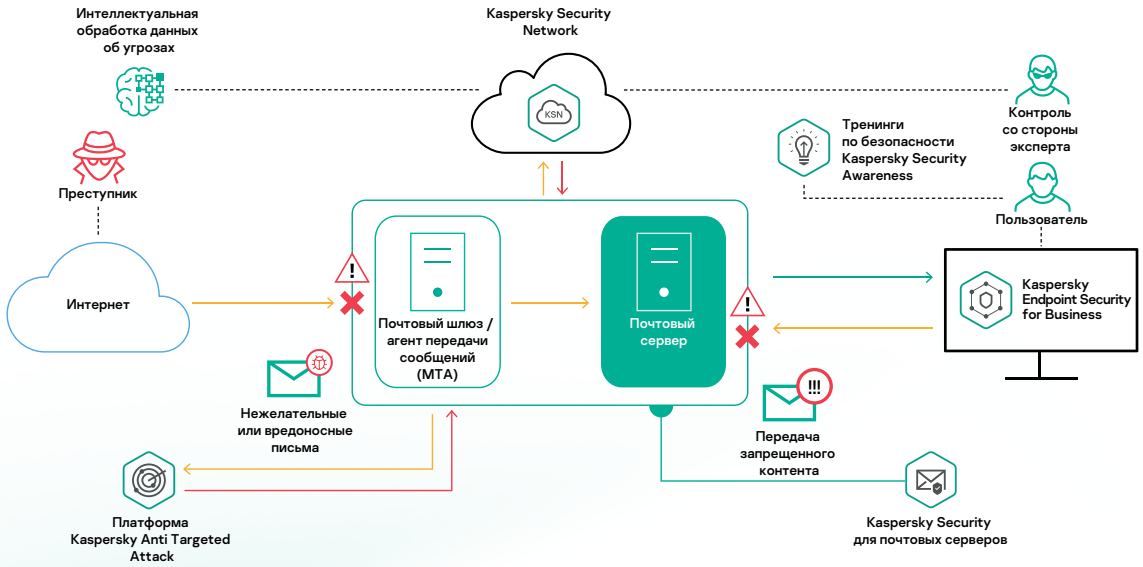
Электронная почта играет ключевую роль в бизнес-коммуникациях. А значит, защита электронной почты должна работать эффективно и не мешать корпоративным коммуникациям. Kaspersky Security для почтовых серверов предлагает самую эффективную защиту от множества угроз (начиная с фишинга и спама и заканчивая компрометацией корпоративной электронной почты и шифровальщиками). Ложные срабатывания минимальны, и ничто не мешает безопасному обмену сообщениями.

Защита электронной почты за пределами шлюза

Kaspersky Security для почтовых серверов выявляет вредоносный и нежелательный контент не только на уровне шлюза, но и на уровне отдельных почтовых ящиков на серверах Microsoft Exchange и Microsoft Exchange Online. Надежная защита почтовых серверов крайне важна для любой компании. Наше решение выявляет и нейтрализует отложенные фишинговые атаки, способные обходить защиту на уровне шлюза, выявляет сообщения злоумышленников, отправленные с электронных адресов ваших сотрудников, и инсайдерские атаки, которые не доходят до шлюза.

Модель атаки через электронную почту

Основные возможности



Предотвращение атак через электронную почту с помощью Kaspersky Security для почтовых серверов

Предотвращение атак через электронную почту с помощью Kaspersky Security для почтовых серверов

Многоуровневая защита на основе самообучающихся нейросетей предотвращает даже самые сложные угрозы, распространяемые через электронную почту, и останавливает шпионские программы, стиратели данных, майнеры и шифровальщики, которые запускаются после успешной направленной фишинговой атаки. Поведенческий анализ, облачные данные о репутации, эвристические и сигнатурные базы данных в сочетании со знаниями экспертов обеспечивают эффективное многоуровневое обнаружение и предотвращение угроз с минимальным количеством ложноположительных срабатываний.

Одна лицензия для многих сценариев

Одна лицензия позволяет использовать решение в самых разных сценариях – как для укрепления защиты существующей почтовой инфраструктуры, так и для создания новой. Наше решение обеспечивает эффективную защиту почтовых серверов на базе Linux или Windows в локальной, виртуализированной, облачной и гибридной средах.

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 на базе машинного обучения с регулярно обновляемыми алгоритмическими моделями и сценариями обрабатывает косвенные индикаторы угроз, чтобы блокировать даже самые убедительные мошеннические письма. Поддержка таких механизмов аутентификации отправителя, как SPF, DKIM и DMARC, защищает от спуфинга. Это особенно важно для предотвращения компрометации корпоративной почты.

Эмуляция в песочнице

Для защиты от самого сложного, 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 в улучшенной внешней песочнице для более глубокой оценки и динамического анализа.

Улучшенная защита от фишинга

Наша улучшенная защита 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 фишинговых угроз и угроз «нулевого часа».

Предотвращение небезопасной передачи контента

Гибко настраиваемая система контентной фильтрации выявляет методы маскировки файлов, которые часто используют злоумышленники, и определяет потенциально опасные вложения. Благодаря функции защиты от потери данных администраторы могут гибко конфигурировать политики безопасности, предотвращающие утечку данных.

Защита почтового ящика за пределами шлюза

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

- **Повторная проверка электронных писем** защищает от отложенной активации фишинговых URL-адресов.
- **Защита от спама с теневым карантином** 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.

Прозрачность

Простой и наглядный веб-интерфейс позволяет администратору управлять защитой и отслеживать ее статус с помощью ряда инструментов:

- настраиваемая панель мониторинга
- удобное средство просмотра и поиска событий с использованием булевых операторов
- экспорт событий в SIEM-систему
- создание отчетов в консоли или их доставка по электронной почте
- диагностики состояния системы

Масштабируемость и отказоустойчивость

Благодаря поддержке кластерной архитектуры решение эффективно справляется с растущим объемом трафика и обеспечивает отказоустойчивость всей системы защиты электронной почты в случае сбоя. Чтобы предотвратить потерю критически важной информации при лечении или удалении зараженных файлов, а также в случае технических неполадок, можно сохранять резервные копии исходных сообщений, отвечающих заданным администратором критериям, чтобы потом безопасно просмотреть их.

Управление и контроль доступа

Благодаря гибкой настройке правил администратор может задавать политики на основе нескольких критериев и отслеживать случаи их нарушения. Единая консоль управления безопасным шлюзом электронной почты позволяет использовать специализированные инструменты для настройки параметров системы, не связанных с безопасностью. Управление доступом на основе ролей дает возможность назначить разных администраторов для разных клиентов или направлений деятельности.

Расширенное обнаружение и реагирование

Благодаря интеграции с платформой Kaspersky Anti Targeted Attack вы получаете доступ к технологиям обнаружения экспертного уровня – улучшенной песочнице, анализатору мобильных угроз, данным о командных серверах и другой информации. Технологии расширенного обнаружения и реагирования, используемые в наших продуктах, способны найти компоненты целевой атаки на разных уровнях инфраструктуры и изолировать их, прервав цепочку поражения.

Роль защиты электронной почты на различных этапах цепочки поражения

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 Server
- Kaspersky Security Center
- Kaspersky Security для Microsoft Office 365 (Exchange Online)