kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Secure Mail Gateway
Шлюз безопасности электронной почты (SEG)

Защита периметра и безопасность коммуникаций

Электронная почта – основной канал, по которому в корпоративные системы проникает вредоносное ПО, угрожающее IT-безопасности бизнеса. Чаще всего злоумышленники используют методы социальной инженерии, чтобы завоевать доверие получателя и мотивировать его сделать то, что делать не рекомендуется.

Kaspersky Secure Mail Gateway – это комплексное решение класса SEG (Secure Email Gateway), способное распознать опасные сообщения электронной почты и заблокировать их прежде, чем они достигнут получателя. Оно не только снижает риск инфицирования и утечки данных, но и экономит время сотрудников, которым приходилось отвлекаться на нежелательную почту.

Особенности Kaspersky Secure Mail Gateway

- Продвинутая защита от вредоносного ПО
- Двусторонняя интеграция с Kaspersky Anti Targeted Attack Platform (KATA)
- Многоуровневая защита от компрометации корпоративной почты (BEC-атак)
- Защита от угроз «нулевого дня»
- Доступ к глобальным аналитическим данным об угрозах в сети Kaspersky Security Network или Kaspersky Private Security Network
- Поддержка Microsoft Active Directory
- Управление доступом на основе ролей
- Защита от внедренных вредоносных макросов и других объектов
- Блокирование шифровальщиков и троянцев-майнеров, распространяемых по электронной почте
- Гибкие возможности масштабирования с учетом нагрузки и размера организации
- Управление карантином для электронных писем и вложений на всех узлах кластера
- Эффективная обработка растущего трафика электронной почты благодаря кластерной архитектуре

Блокирование атак по электронной почте на ранней стадии

Kaspersky Secure Mail Gateway эффективно борется с фишингом, попытками компрометации корпоративной электронной почты, шифровальщиками и даже продвинутыми атаками по электронной почте. Безопасный шлюз действует на ранних этапах цепочки поражения, пока угрозы не привели к инцидентам и не причинили ущерба. Благодаря этому эффективно снижается риск атаки, а сотрудники не отвлекаются на ненужную дополнительную работу. Интеллектуальная обработка данных осуществляется на всех уровнях защиты, подкрепленных технологией машинного обучения. Применение разных моделей машинного обучения, песочницы и облачной репутационной системы позволяет нам правильно фильтровать сообщения электронной почты, отделяя нужные от опасных.

Повышение продуктивности за счет блокирования спама

Интеллектуальные компоненты защиты от спама минимизируют число ложных срабатываний и адаптируются 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.

Усиление защиты с минимальными трудозатратами

Приложение поставляется в виде готового программного устройства, простого в развертывании и настройке. Оно подойдет как компаниям, желающим добавить SEG-решение в свою почтовую инфраструктуру, так и тем, кто намерен повысить эффективность защиты используемых почтовых систем.

Масштабирование защиты по мере развития бизнеса

Масштабируемая кластерная архитектура Kaspersky Secure Mail Gateway позволяет расширять возможности защиты по мере необходимости. Вам не придется жертвовать производительностью, чтобы поддерживать высокий уровень безопасности электронной переписки вашего растущего бизнеса.

Роль защиты электронной почты на различных этапах цепочки поражения

Основные возможности

На основе разработок всемирно признанной команды экспертов

Уникальный опыт экспертов «Лаборатории Касперского» в области противодействия новым угрозам и создания инновационных решений безопасности признан во всем мире. Они принимали участие в борьбе с такими преступными группировками, как Carbanak и Stuxnet, Duqu и Equation, Lazarus и MosaicRegressor. Большинство атак начинаются с электронной почты и наши эксперты подробно изучают и анализируют инструменты преступников. Результаты такой работы закладывают основу для дальнейшего развития технологий обнаружения. Наши решения регулярно участвуют во внутренних и внешних тестированиях с самыми высокими требованиями и мы неизменно опережаем наших конкурентов.

См. страницу
https://www.kaspersky.ru/top3

Многоуровневая защита от вредоносного ПО

Продвинутая защита от вредоносного ПО включает несколько проактивных уровней и использует как локальные модели машинного обучения, так и облачную аналитику угроз для выявления во входящей почте вредоносных вложений и программ – как известных, так и новых.

Глобальная аналитика угроз. Kaspersky Secure Mail 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 и поведенческий анализ в песочнице. 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.

Kaspersky Security Network / Private Security Network. Для оперативного блокирования новейших видов спама, фишинга и вредоносного ПО необходима актуальную информацию об угрозах. Kaspersky Security Network предоставляет самую свежую аналитику, дополненную телеметрическими данными об обнаруженных угрозах по всему миру, результатами исследований антивирусных экспертов и информацией, полученной от партнеров и из других источников. Kaspersky Private Security Network защищает инфраструктуру организаций, предъявляющих самые высокие требования к конфиденциальности, и предотвращает даже малейшую утечку корпоративной информации.

Обнаружение скриптов. По данным аналитиков информационной безопасности, скрипты все чаще используются для атак по электронной почте и встраивания вредоносного ПО в безобидные с виду офисные файлы. Kaspersky Secure Mail Gateway нейтрализует опасные скрипты, в том числе макросы Microsoft Office, обеспечивает эффективное противодействие подобным угрозам.

Проверка архивов. Создатели вредоносных программ часто архивируют вложения перед отправкой потенциальной жертве. Решения «Лаборатории Касперского» могут обнаружить угрозу даже в многоуровневых архивах.

Готовое к использованию решение

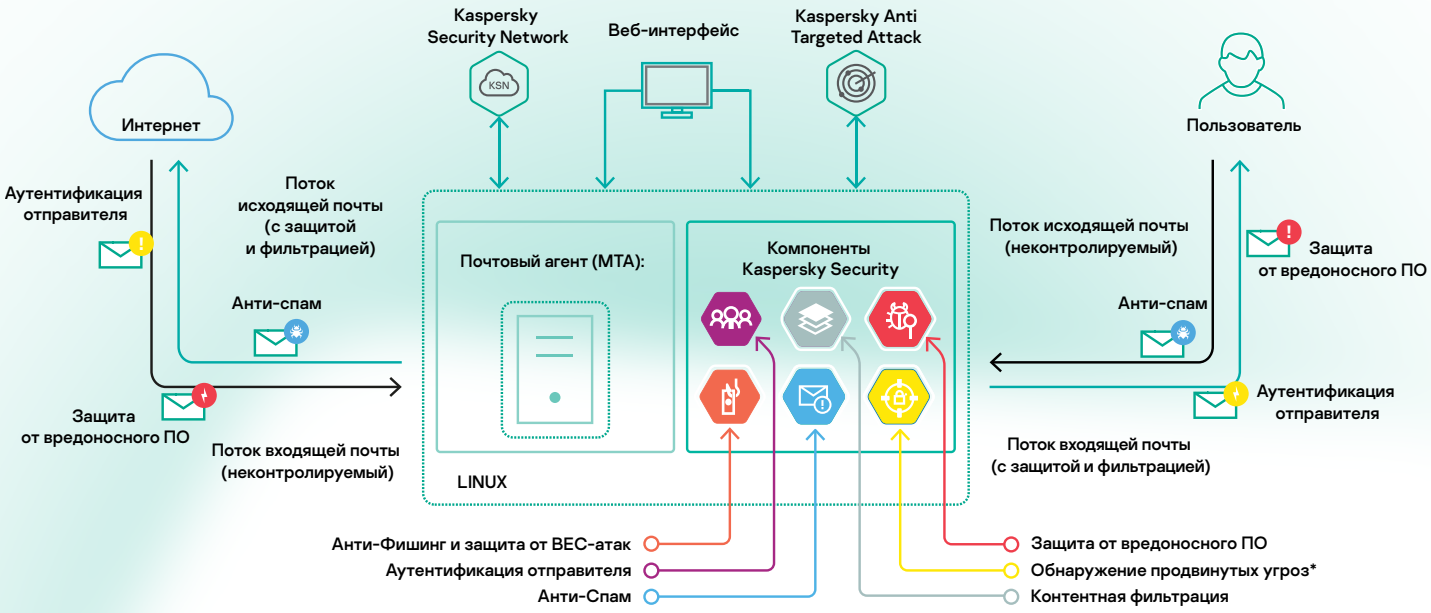
Полнофункциональное программное устройство. В Kaspersky Secure Mail Gateway входят все необходимые компоненты для создания безопасной почтовой инфраструктуры, включая ОС на базе Linux, агент доставки почты (MTA), защитное приложение «Лаборатории Касперского» и т. д. Решение легко интегрируется с другими компонентами. Администратору нужно изменить лишь несколько параметров конфигурации.

Поддержка платформ виртуализации. Решение Kaspersky Secure Mail Gateway реализовано в форме образа виртуальной машины, совместимого с самыми популярными платформами виртуализации. Их можно скачать в виде образа и развернуть как рабочую нагрузку (workload) в облаке или корпоративном датацентре.

Защита от спама (без потери нужной информации)

Ультрасовременная защита от спама (с контентной фильтрацией на основе репутации). Система защиты от спама, разработанная «Лабораторией Касперского», широко использует модели обнаружения на основе машинного обучения. Эксперты «Лаборатории Касперского» контролируют автоматизированную обработку спама, чтобы свести к минимуму вероятность ложных срабатываний и адаптироваться к изменениям в ландшафте угроз. Данные о репутации, поступающие из базы Kaspersky Security Network, гарантируют точное обнаружение новых видов спама сразу же после их появления в интернете.

Защита от спама с карантином. В неоднозначных случаях подозрительные письма можно поместить на временный карантин, пока Kaspersky Security Network не соберет достаточно данных, чтобы определить, безопасны ли они. Спам отправляется в специальное хранилище – это гарантирует, что ни одно важное письмо не потеряется. Администратор может настроить параметры электронных писем, которые необходимо помещать на карантин, и срок их хранения – это позволит восстановить важные сообщения и переслать их адресату в неизменном виде.



* В составе Kaspersky Anti Targeted Attack

Атаки с использованием похожих доменов

При использовании похожих доменов (lookalike-атаки) маскируется адрес отправителя. Злоумышленники регистрируют домен, который очень похож на легитимный, доверенный домен. Символы Юникода могут заменяться другими, похожими на них.

Преступники нередко используют домены третьего уровня, например kaspersky.xxx.com, злоупотребляя доверием пользователей к популярному бренду или бизнес-партнеру.

Эксплуатация уязвимостей почтовых клиентов

В арсенале злоумышленников есть целый набор инструментов для эксплуатации некоторых уязвимостей распространенных почтовых клиентов и операционных систем. Они объединены под общим названием Mailsploit и дают возможность подменить адрес отправителя, пользуясь уязвимостью некоторых почтовых клиентов.

При этом, разработчики ряда почтовых клиентов знают об этих свойствах своих продуктов - и не торопятся их исправлять, считая их частью задуманной функциональности и предлагая решить проблему на уровне шлюза.

Как только создатель коллекции Mailsploit открыл исходный код широкой публике, спамеры и хакеры взяли ее на вооружение – чего и следовало ожидать. Коллекция стала использоваться для атак на системы, владельцы которых пренебрегают защитой и установкой исправлений.

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».

Защита от специализированных BEC-атак

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. Решение обнаруживает атаки с использованием похожих доменов, кражу учетных записей, эксплуатацию уязвимостей почтовых клиентов и другие типы угроз.

Управление электронной почтой с проверкой подлинности

Надежные механизмы аутентификации отправителя, такие как SPF/DKIM/DMARC, помогают обеспечить защиту от атак через ложные серверы. Это особенно важно для борьбы с BEC-атаками.

Категории электронной почты

В решении уже задано несколько категорий электронной почты для фильтрации сообщений, что упрощает повседневную обработку потоков почты и снижает риски безопасности.

Популярность направленного фишинга

APT-группировка Sofacy (также известная как APT28 и Fancy Bear) прославилась проведением сложнейших кибератак. Она использует многочисленные сценарии направленного фишинга и компрометации корпоративной почты – от укороченных ссылок на вредоносные сайты, крадущие учетные данные, до эксплойтов нулевого дня, встроенных во вложенные офисные документы.

Источник: Securelist

Фильтрация вложений

Некоторые типы вложений лучше не пропускать в корпоративный периметр безопасности – это слишком опасно. Разработанная «Лабораторией Касперского» система фильтрации обеспечивает гибкую настройку политики доставки вложений и распознает множество методов маскировки файлов, которые часто используются киберпреступниками. Эти функции помогают снизить риск утечки данных.

Управление и прозрачность

Удобная веб-консоль. Простой в использовании веб-интерфейс позволяет администратору контролировать состояние защиты электронной почты и настраивать правила и политики. Для каждого контролируемого домена можно настроить отдельные наборы правил.

Широкие возможности управления событиями. Средство просмотра событий предоставляет администратору всю необходимую информацию. Для поиска нужных данных можно задать критерии любого уровня сложности с использованием логических (булевых) операторов.

Интеграция с SIEM-системами. Благодаря поддержке общего формата событий (CEF), можно экспортировать информацию о событиях безопасности в почте в корпоративную SIEM-систему и отслеживать оповещения системы безопасности электронной почты в общем контексте безопасности.

Система управления доступом на основе ролей. Для ограничения прав различных категорий администраторов можно настроить отдельные роли. Такая система полезна для делегирования задач внутри компании и дает нужную степень контроля клиентам поставщиков управляемых услуг (MSP).

Гибкая настройка правил. Тонкая настройка политик безопасности делает решение максимально эффективным в контексте бизнес-процессов вашей компании. В Kaspersky Secure Mail Gateway реализована простая и гибкая система настройки правил, которая позволяет детально управлять безопасностью электронной почты. При этом администраторам не придется тратить много времени на ее изучение.

Интеграция с Active Directory. Kaspersky Secure Mail Gateway может получать информацию об объектах корпоративного домена (пользователях, группах пользователей, компьютерах и т. д.) для настройки правил доступа на основе ролей и политик безопасности в отношении известных объектов, работающих в вашей IT-сети. Между приложением и Active Directory постоянно выполняется синхронизация данных, описывающих объекты, с учетом последних изменений в корпоративной инфраструктуре.

Кластерная архитектура. В основе решения лежит кластерная архитектура, которую можно масштабировать по мере роста вашего бизнеса и увеличения трафика электронной почты – защита не потеряет своей эффективности.

Интеграция с платформой Kaspersky Anti-Targeted Attack

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. Самые изощренные вредоносные письма, обнаруженные механизмами Kaspersky Anti Targeted Attack, отправляются на карантин.

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. Управление резервным копированием осуществляется централизованно из единой консоли управления.

www.kaspersky.ru