kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky® Web Traffic Security

Стратегическая защита от веб-угроз

Kaspersky Web Traffic Security защищает корпоративные сети от веб-угроз, снижает риск утечки данных и повышает производительность труда за счет управления доступом к интернет-ресурсам. Широкие возможности, универсальность и скорость реагирования позволяют этому приложению обеспечивать своевременную и эффективную защиту в самых разных корпоративных сценариях..

Особенности

- Многоуровневая защита от вредоносного ПО и фишинга
- Защита от угроз «нулевого часа»
- Контентная и репутационная фильтрация
- Блокирование вирусов-вымогателей
- Веб-Контроль
- Масштабируемость для использования в сетях с высокой нагрузкой
- Интеграция с Kaspersky Security Network
- Доступ к администрированию и интернету на основе ролей
- Поддержка Microsoft Active Directory
- Поддержка рабочих областей для компаний с распределенной структурой
- Поставляется в виде отдельного приложения или готового к использованию программного устройства безопасности
- Интеграция с решением для защиты от целевых атак Kaspersky Anti Targeted Attack для автоматического реагирования на угрозы

Ключевые преимущества

Снижение риска заражения благодаря сочетанию защиты и контроля

Kaspersky Web Traffic Security блокирует входящие угрозы на уровне шлюза и не позволяет им достигать рабочих мест. Это значительно снижает вероятность эксплуатации уязвимостей и атак на основе методов социальной инженерии. Также приложение помогает контролировать и ограничивать использование интернет- ресурсов, минимизируя количество теневых IT-операций и инцидентов, связанных с ошибками пользователей.

Повышение эффективности защиты корпоративного шлюза

Благодаря мощным технологиям защиты, высокой скорости обнаружения угроз и минимальному количеству ложных срабатываний Kaspersky Web Traffic Security значительно повышает эффективность используемых средств защиты шлюза. Кроме того, приложение легко интегрируется с другими решениями «Лаборатории Касперского».

Адаптация к индивидуальным потребностям

Приложение хорошо масштабируется, подстраиваясь под потребности организации и структуру корпоративной сети, поддерживает иерархическое развертывание, управление несколькими узлами и клиентами, а также контроль и делегирование доступа на основе ролей.

Отдельное приложение или программное устройство	Вы можете выбрать, какой вариант установки: развертывание виртуального образа, содержащего готовый прокси-сервер и систему его защиты, или установка приложения для обеспечения безопасности существующего в сети прокси-сервера

Возможности

Многоуровневая защита от угроз

Новейшие средства обеспечения безопасности и контроля, разработанные «Лабораторией Касперского», включают в себя несколько уровней проактивной защиты.

Защита от вредоносного ПО

Проактивные технологии обнаружения на основе машинного обучения, анализ и фильтрация выявляют и блокируют вредоносное ПО (такое как шпионские программы, банковские троянцы, программы-вымогатели, криптомайнеры).

Обнаружение новых угроз в режиме реального времени

Облачная сеть Kaspersky Security Network, постоянно обновляемая на основе данных наших экспертов и десятков миллионов пользователей по всему миру, помогает обнаруживать потенциальные угрозы по мере их появления – в режиме реального времени – с минимальным количеством ложных срабатываний.

Эмуляция в песочнице

Вложения выполняются и анализируются в безопасной эмулируемой среде – таким образом обеспечивается защита даже от сложного, тщательно замаскированного вредоносного ПО.

Обнаружение скриптов

Приложение обнаруживает и блокирует скрипты, встраивающие вредоносное ПО в файлы, на первый взгляд не представляющие опасности, а также используемые в атаках со скрытой загрузкой.

Репутационная фильтрация

Репутация файлов и адресов, постоянно обновляемая на основе облачных баз Kaspersky Security Network, позволяет блокировать подозрительные или нежелательные файлы и интернет-ресурсы без проведения глубокого анализа.

Передовая защита от фишинга

Модели обнаружения используют облачную защиту от известных и неизвестных фишинговых угроз и угроз «нулевого часа» на базе нейросетевого анализа более чем по 1000 критериев. Они включают анализ изображений, языковые проверки и специфические скрипты, а также собираемые со всего мира данные о вредоносных и фишинговых веб и IP-адресах.

Контентная фильтрация

Передачу потенциально проблемных или нежелательных типов файлов можно запретить на основе таких параметров, как имя, расширение (для обнаружения файлов с поддельными расширениями используется компонент Format Recognizer), размер, тип MIME (видео, изображения и т. д.) и хеш.

Контроль доступа в интернет

Администраторы могут создавать правила, блокирующие доступ к веб-ресурсам на основе предопределенных категорий или собственных списков. Таким образом снижаются риски для безопасности, а пользователи перестают отвлекаться на посторонние сайты. При необходимости можно применить сценарий «Запрет по умолчанию», ограничивающий доступ к веб-ресурсам, которые не являются необходимыми для работы пользователя или группы.

Гибкая интеграция

Благодаря высокой адаптивности и практически неограниченной масштабируемости приложение Kaspersky Web Traffic Security легко интегрируется в существующую IT-инфраструктуру.

Безопасность систем с поддержкой ICAP
Безопасность трафика обеспечивается на любом устройстве, поддерживающем протокол ICAP, а не только на прокси-серверах.

Двусторонняя интеграция с Kaspersky Anti Targeted Attack

Интеграция с системой обнаружения целевых атак предоставляет дополнительные данные для углубленного анализа продвинутых угроз и позволяет автоматически блокировать компоненты атак и действия злоумышленников через интернет, например передачу команд и вредоносного кода, а также извлечение украденных данных.

Интеграция с SIEM-системами
Приложение расширяет возможности систем управления данными и событиями безопасности (SIEM) с помощью экспорта информации в общий формат событий (CEF).

Гибкое управление

Единая консоль управления

Управление безопасностью всех систем осуществляется из единой веб-консоли. Таким образом повышается прозрачность и управляемость инфраструктуры. Консоль также отражает результаты анализа угроз с акцентом на события безопасности и содержат данные о текущей активности. Доступна возможность анализа поведение пользователей в интернете.

Интеграция с Active Directory

Обеспечивает конфигурирование и постоянную синхронизацию правил доступа на основе ролей и политик безопасности с вашей сетью и инфраструктурой.

Контроль доступа на основе ролей

Можно определять различные административные роли со своими правами и ограничениями. Это облегчает делегирование внутренних задач и предоставление надлежащего уровня контроля клиентам сервисов.

Поддержка рабочих областей

Выделяйте рабочие области для различных подразделений и филиалов и управляйте ими по отдельности, при необходимости комбинируя глобальные и локальные политики.

Варианты развертывания

Kaspersky Web Traffic Security может быть интегрирован в корпоративную сеть в качестве системы защиты существующего прокси-сервера. Второй вариант позволяет развернуть полноценное программное устройство безопасности, включающее готовый к использованию прокси-сервер и систему его защиты.

КАК ПРИОБРЕСТИ

Kaspersky Web Traffic Security входит в состав Kaspersky Security для интернет-шлюзов и Kaspersky Total Security для бизнеса. Чтобы выбрать подходящее решение, обратитесь к компании-партнеру в вашем регионе : (**http://kaspersky.ru/find_partner_office**)

www.kaspersky.ru