Kaspersky® Web Traffic Security

Стратегическая защита всей сети

Прокси-сервер расположен стратегически выгодно: будучи узким местом всего трафика между корпоративной инфраструктурой и внешней средой этот шлюз предоставляет отличную возможность минимальными усилиями сдерживать угрозы на ранних этапах.

Kaspersky Web Traffic Security – это приложение, которое в интеграции с интернет-шлюзами (прокси-серверами) обеспечивает защиту корпоративной IT-сети от интернет-угроз и повышает производительность труда за счет управления доступом к внешним ресурсам. Решение обрабатывает веб-трафик, проходящий через прокси-сервер, и блокирует все, что представляет опасность с точки зрения корпоративной политики. Несмотря на стандартный подход к защите периметра, Kaspersky Web Traffic Security выгодно отличается от других доступных предложений благодаря широкому спектру возможностей и высокому качеству защиты.

Основные возможности

- Защита нового поколения от вредоносных программ и фишинга в режиме реального времени и по запросу
- Фильтрация содержимого для блокирования подозрительных файлов и предотвращения утечки данных
- Масштабируемость
- Защита от угроз «нулевого часа»
- Интеграция с Kaspersky Security Network
- Поддержка Microsoft Active Directory
- Ролевой доступ для администрирования и доступа к интернету
- Рабочие области для создания политик по подразделениям компании
- Контроль использования веб-ресурсов
- Блокирование программ-шифровальщиков при попытке проникновения в сеть
- Мониторинг доступа в сеть, возможность расследования инцидентов

Преимущества

Предотвращает нарушение бизнес-процессов

Останавливая большинство входящих угроз на уровне интернет-шлюза и не позволяя им достигать рабочих мест, Kaspersky Web Traffic Security существенно снижает нагрузку на средства защиты рабочих станций, а также уменьшает влияние человеческого фактора.

Сокращает расходы IT- и ИБ-отделов

Даже при использовании эффективной системы защиты рабочих мест, чем реже она будет сообщать об опасности, тем меньше будет волнений среди сотрудников и тем меньше времени будет уходить на расследование инцидентов.

Повышает производительность труда

Благодаря управлению использованием интернет-ресурсов Kaspersky Web Traffic Security не только уменьшает угрозу кибератак, но и ограничивает отвлекающие факторы, а также сокращает возможность использования нежелательных ресурсов. Особенно это актуально при наличии в сети устройств на платформах, отличных от Windows®.

Масштабируется в соответствии с размером компании

Решение можно масштабировать в зависимости от загруженности конкретной системы, чтобы поддерживать управление несколькими узлами и иерархическое развертывание.

Снижает риски, связанные с передачей определенных типов файлов

Kaspersky Web Traffic Security повышает безопасность за счет запрета на передачу файлов определенных типов. Это позволяет предотвратить заражение вредоносным содержимым, встроенным в документы, а также снизить риск утечки данных. Запрет на загрузку медиафайлов и страниц с развлекательным контентом для пользователей, которым они не требуются для работы, также способствует росту производительности труда.

Основные функции

Многоуровневая защита от различных видов киберугроз

Защита нового поколения включает несколько уровней проактивной защиты, в том числе основанных на алгоритмах машинного обучения и использовании облачных технологий. Решение обеспечивает блокирование вредоносного ПО, программ-шифровальщиков и потенциально нежелательных приложений во входящем и исходящем трафике.

Машинное обучение

Глобальная аналитика угроз с использованием больших данных (big data) опирается на сочетание мощных алгоритмов машинного обучения с опытом экспертов. Результатом является высокий уровень обнаружения угроз при минимальном количестве ложных срабатываний.

Эмуляция в песочнице

Для защиты от самого сложного и тщательно замаскированного вредоносного ПО вложения запускаются и анализируются в безопасной среде. Поэтому опасные экземпляры не попадают в корпоративную систему.

Обнаружение скриптов

Согласно данным аналитиков по информационной безопасности, скрипты все чаще используются для атак через интернет и встраивания вредоносного ПО в безобидные с виду офисные файлы. Kaspersky Web Traffic Security помогает в обоих случаях, предотвращая атаки с попутной загрузкой и выполнение опасных программ еще до того, как они попадут на конечное устройство.

База данных узлов, связанных с кибератаками

Для предотвращения малейшей угрозы взаимодействия с опасными ресурсами этот облачный сервис проверяет запрашиваемый ресурс по обширной базе данных активных командных серверов киберпреступников, объектов с угрозами «нулевого дня», заражающих устройства веб-сайтов и точек распространения вредоносных программ, которые, по нашим данным, нацелены на взлом. Эта база данных постоянно обновляется в режиме реального времени с использованием аналитических данных, предоставляемых глобальным центром исследований и анализа угроз «Лаборатории Касперского», что позволяет до выполнения запроса блокировать даже самые новые опасные ресурсы.

Сервис веб-репутации

Kaspersky Web Traffic Security включает репутационный сервис (Kaspersky Reputation Service), который обрабатывает запросы о репутации файлов, ссылок и IP-адресов, используя как данные облачной базы Kaspersky Security Network, так и локальные базы решения. Это позволяет моментально блокировать подозрительные и нежелательные файлы и веб-ресурсы.

HuMachine™ – новый подход к разработке технологий защиты

Система HuMachine Intelligence™ отражает подход «Лаборатории Касперского» к защите бизнеса от неизвестных и сложных угроз.

В основе этой концепции лежат три взаимосвязанных компонента: обработка больших данных об угрозах, алгоритмы машинного обучения и многолетний опыт экспертов компании.

Решения «Лаборатории Касперского» для защиты бизнеса содержат целый спектр технологий нового поколения, в том числе интеллектуальный анализ поведения и алгоритмы машинного обучения.

Для повышения эффективности обнаружения предлагаемая «Лабораторией Касперского» улучшенная защита от фишинга опирается на нейросетевой анализ. Она использует более тысячи критериев, включая анализ изображений, языковые проверки и сигнатуры скриптов, и опирается на собираемые со всего мира данные о вредоносных и фишинговых URL-адресах для защиты как от известных, так и от неизвестных фишинговых URL-адресов и угроз «нулевого часа», содержащихся в загружаемых файлах. В этом помогают облачные технологии.

Контентная фильтрация

Решение позволяет запретить передачу файлов определенных типов. Для фильтрации можно использовать множество параметров, включая имя, расширение/тип (для файлов с поддельными расширениями используется распознавание формата), размер, тип MIME и хэш. Контентную фильтрацию можно использовать в различных целях, включая снижение угрозы кибератак, предотвращение утечки данных, уменьшение объема трафика и повышение производительности.

Веб-контроль с использованием категорий

Для работы сотрудникам требуются далеко не все веб-ресурсы, а многие могут представлять реальную угрозу для безопасности и репутации компании (например, если на них будут размещены вредоносные или пиратские программы). Веб-контроль позволяет ограничить определенные категории веб-ресурсов для снижения рисков и обеспечения бесперебойной работы без нежелательных помех. В случае необходимости можно использовать сценарий «Запрет по умолчанию», ограничивающий использование всех веб-ресурсов, кроме тех, которые действительно нужны для работы отдельного сотрудника или группы.

В решении также реализован механизм блокирования ресурсов, запрещенных законодательством Российской Федерации (ФЗ-114, -139, -152, -436).

Контроль трафика с SSL-шифрованием

Архитектура решения позволяет легко реализовать контроль корпоративного трафика (corporate traffic surveillance). Сейчас, когда веб-трафик с SSL-шифрованием фактически становится стандартом в интернете, эта возможность просто необходима.

Безопасность систем с поддержкой ICAP

Помимо прокси-серверов решение «Лаборатории Касперского» можно использовать для защиты трафика любого устройства, поддерживающего протокол ICAP.

Интеграция с SIEM-системами

Если в компании для отслеживания активности в корпоративной сети используется система управления данными и инцидентами безопасности (SIEM-система), Kaspersky Web Traffic Security расширит ее возможности с помощью экспорта информации в общий формат событий (CEF) вместе с широко используемым системным журналом.

Простое администрирование

В решении Kaspersky Web Traffic Security реализована гибкая и простая система управления.

Управление безопасностью всех систем с поддержкой ICAP, включая прокси-серверы и хранилища, происходит посредством единого веб-интерфейса: администраторам доступны широкие возможности управления и обеспечения прозрачности.

Удобная панель управления

Все, что требуется для контроля текущего состояния корпоративной безопасности на уровне шлюза, собрано на единой панели управления, которая мгновенно предоставляет полный обзор ситуации, включая экстренные события. Также консоль обеспечивает возможность простого контроля работы всех составляющих кластера системы.

Управление событиями

Результаты анализа угроз представляются с ориентацией на события и отображением активности в режиме реального времени. Кроме того, можно анализировать поведение пользователей в интернете.

Гибкая система конфигурирования правил

Решение позволяет не только обеспечивать безопасность на нескольких уровнях, но и тонко настраивать политики безопасности в соответствии с используемыми бизнес-процессами – это дополнительно повышает его эффективность. В решении Kaspersky Web Traffic Security реализована гибкая и простая система конфигурирования правил, которая позволяет детально управлять безопасностью шлюза. При этом администраторам не придется тратить много времени на ее изучение.

Система управления доступом на основе ролей

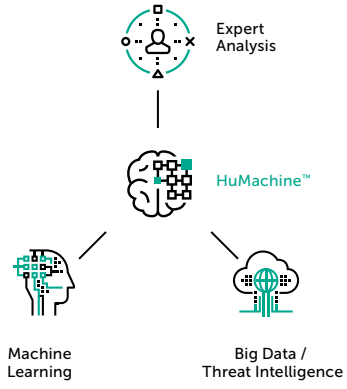
Администраторы могут определять роли для ограничения прав различных категорий администраторов. Эта система полезна для делегирования задач внутри компании. Кроме того, она позволит поставщикам управляемых услуг предоставлять своим клиентам необходимые им возможности управления и контроля.

Интеграция с Active Directory

Kaspersky Web Traffic Security может получать информацию об объектах корпоративного домена (пользователи, группы пользователей, компьютеры и так далее) для конфигурирования правил доступа на основе ролей и политик безопасности в отношении известных объектов, работающих в IT-сети компании. Данные, описывающие объекты, постоянно синхронизируются между приложением и Active Directory, чтобы учитывались последние изменения в корпоративной инфраструктуре.

Поддержка нескольких клиентов

Специальный режим для поставщиков IT-услуг (IT-аутсорсинг) и многоотраслевых компаний позволяет назначать особые области («рабочие пространства») для различных подразделений или компаний-клиентов и управлять ими отдельно с использованием требуемой комбинации «глобальных» и «локальных» политик.



«Лаборатория Касперского»

www.kaspersky.ru

#истиннаябезопасность
#HuMachine