Kaspersky Private Security Network

Локальная репутационная база угроз для изолированных сетей

При использовании традиционных сигнатурных методов защиты на нейтрализацию угрозы может уйти несколько часов. В то же время, по данным «Лаборатории Касперского», ежедневно появляется более 300 000 новых вредоносных программ. Для повышения уровня безопасности в условиях изолированных сетей и жестких требований к системе защиты «Лаборатория Касперского» предлагает Kaspersky Private Security Network (KPSN) — локальную версию облачной репутационной базы угроз Kaspersky Security Network.

Вы получаете все преимущества облачной сети безопасности, но без передачи данных за пределы локальной сети и без нарушений требований IT-безопасности для изолированных сетей.

Выполняемые задачи

- Доступ в режиме реального времени к статистике угроз и репутации объектов
- Противодействие распространению вредоносного ПО
- Снижение рисков и минимизация ущерба от инцидентов кибербезопасности
- Снижение риска ложных срабатываний
- Возможность обогащения «вердиктами» заказчика
- Соблюдение нормативных требований по обеспечению безопасности изолированных сетей

Ключевые преимущества

- Уникальные сведения о новейших и наиболее сложных атаках, предоставляемые в рамках контролируемой среды вашей локальной сети
- Открытый API для доступа к базе KPSN по протоколу HTTP
- Адаптация решения к условиям полной изоляции сети по методу «воздушного зазора» (air gap)
- Гибкие возможности развертывания и тестовый режим
- Нормативно-правовое соответствие требованиям регуляторов и стандартов изоляции высококритичных сетей
- Сертификация ФСТЭК (тип «А» второго класса защиты) совместно с центром управления Kaspersky Security Center
- Поддержка сертифицированной ОС Astra Linux v1.4
- Повышение эффективности защитных решений «Лаборатории Касперского» благодаря оперативному оповещению об угрозах и минимизации ложных срабатываний

Kaspersky Private Security Network оценят по достоинству:

- Крупные компании, предъявляющие строгие требования к защите информации
- Государственные организации
- Телекоммуникационные компании
- Энергетические и промышленные предприятия с физически изолированными сетями
- Предприятия с критически важной инфраструктурой
- Сервис-провайдеры

Системные требования

Для установки компонента KPSN требуется выделенный сервер с соответствующими аппаратными требованиями:

- 8-ядерный процессор 2 ГГц
- 96 ГБ оперативной памяти (RAM)
- 600 ГБ свободного места на твердотельном накопителе (SSD)
- Скорость сетевого подключения 100 Мбит/с

Программные требования:

- Astra Linux® v1.4 или RHEL 7.2/ CentOS 7.2
- Браузер Google Chrome™, Mozilla® Firefox® или Opera
- Java-плагин версии 7 или выше

Поддержка изолированной работы Kaspersky Anti Targeted Attack Platform

Для корректной работы с решением Kaspersky Anti Targeted Attack Platform базе KPSN требуются дополнительные данные, размещаемые на дополнительно выделяемом сервере, аналогичной конфигурации с основным.

Автоматический анализ на основе репутации и поведения

Kaspersky Private Security Network предоставляет решениям «Лаборатории Касперского» необходимую для анализа информацию о репутации файла по его хеш-сумме, в том числе: вердикт, категорию, цифровую подпись и степень популярности.

Кроме того, локальная репутационная база предоставляет сведения и о безопасных, и о вредоносных онлайн-ресурсах и распознает аномальное поведение программ, которое может свидетельствовать о вредоносной активности.

Без права передачи

Kaspersky Private Security Network — это программный продукт, размещаемый на физических или виртуальных мощностях в инфраструктуре организации. Для того чтобы базы данных об угрозах всегда находились в актуальном состоянии, Kaspersky Private Security Network поддерживает одностороннюю связь с сервером облачной репутационной сети Kaspersky Security Network: получает обновления, но не передает данные и не формирует запросов.

Защита изолированных сред

Решение может применяться даже в физически изолированных средах или средах, где действует запрет на передачу данных вовне. В этом случае предусмотрен вариант промежуточного шлюза KPSN, который может быть размещен в сегменте с доступом в интернет (например, в DMZ). Обновления при этом устанавливаются через съемные устройства или с помощью средств однонаправленной передачи данных. Таким образом, предприятие получает новейшие сведения об угрозах в рамках принятых политик безопасности и без изменения существующей инфраструктуры.

Рещения для защиты крупного бизнеса:
kaspersky.ru/enterprise

#ИстиннаяБезопасность