KASPERSKY PRIVATE SECURITY NETWORK

Локальная репутационная база угроз для изолированных сетей со специфическими требованиями к IT-безопасности

При использовании традиционных сигнатурных методов защиты на нейтрализацию угрозы может уйти несколько часов. В то же время, по данным «Лаборатории Касперского», ежедневно появляется более 310 000 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 .

Решение Kaspersky Private Security Network можно установить в центре обработки данных организации, и его работу будут полностью контролировать IT-специалисты вашего предприятия. Вы получаете все преимущества облачной сети безопасности, но без передачи данных за пределы локальной сети, не подвергая при этом риску сохранность конфиденциальных данных и не нарушая требования IT-безопасности для изолированных сетей.

ВЫПОЛНЯЕМЫЕ ЗАДАЧИ

- Предотвращение распространения вредоносного ПО
- Минимизация ущерба от инцидентов кибербезопасности
- Снижение риска ложных срабатываний
- Определение характера атак и отделение целевых атак от массовых угроз
- Расследование инцидентов и устранение последствий
- Соблюдение нормативных требований по обеспечению безопасности изолированных сетей

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

Физической изоляции больше недостаточно

Закрытым инфраструктурам раньше не требовалось получать актуальные данные об угрозах, но сегодня ситуация изменилась: даже физической изоляции от внешних сетей уже недостаточно для полной защиты, так как вредоносное ПО может попасть в сеть, например, с помощью одного зараженного USB-накопителя. KPSN переносит преимущества облачной репутационной сети в закрытые инфраструктуры.

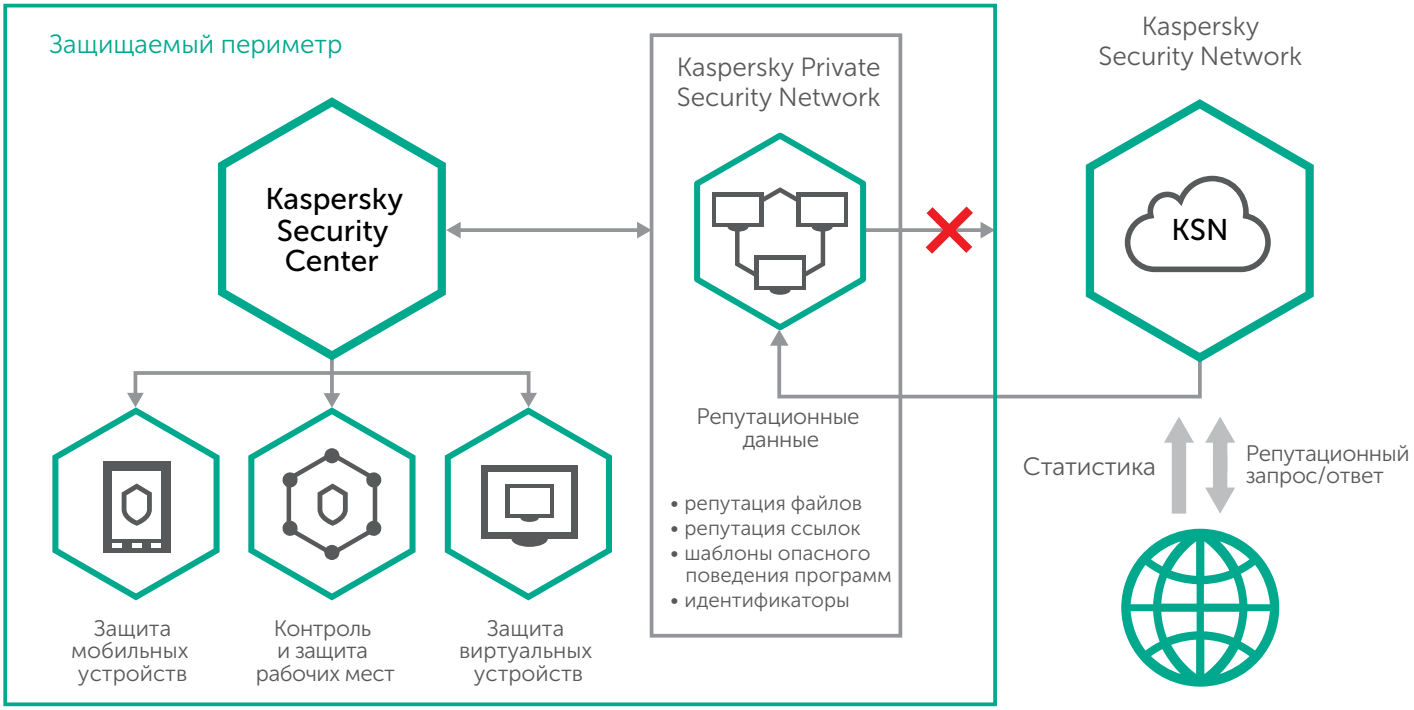
Ключевые преимущества

- Уникальные сведения о новейших и наиболее сложных атаках, предоставляемые в рамках контролируемой среды вашей локальной сети
- Адаптация решения к условиям изолированной сети
- Гибкие возможности развертывания и тестовый режим
- Соответствие требованиям к обеспечению безопасности и защите конфиденциальных данных
- Нормативно-правовое соответствие требованиям регуляторов и стандартов изоляции высококритичных сетей
- Высокий уровень защиты благодаря быстрой реакции на угрозы и минимизации ложных срабатываний

Автоматический анализ на основе репутации и поведения

Kaspersky Private Security Network предоставляет всю необходимую для анализа информацию о репутации файла по его хеш-сумме, в том числе: вердикт, категорию, цифровую подпись и степень популярности. Вердикты и категории файлов регулярно синхронизируются с регулярно обновляемыми динамическими белыми списками «Лаборатории Касперского».

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.



СИСТЕМНЫЕ ТРЕБОВАНИЯ

Kaspersky Private Security Network (KPSN) представляет собой программное решение, состоящее из двух компонентов, которые устанавливаются на физические или виртуальные серверы:

- Репутационная база файлов и URL-ссылок
- Сервисный сервер KPSN

Для установки компонента KPSN требуется выделенный сервер, соответствующий указанным ниже требованиям.

Аппаратные требования:

- 4-ядерный процессор 3,3 ГГ
- 256 ГБ оперативной памяти (RAM)
- 300 ГБ свободного места на жестком диске (HDD)
- Скорость сетевого подключения 1 Гбит/с

Программные требования:

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

ПОДРОБНЕЕ:
http://www.kaspersky.ru/kpsn

Архитектура Kaspersky Private Security Network

БЕЗ ПРАВА ПЕРЕДАЧИ

Kaspersky Private Security Network — это программный продукт, размещаемый на физических серверах 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 прием любых данных извне. 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 однонаправленного соединения с интернетом. Таким образом, предприятие получает новейшие сведения об угрозах в рамках принятых политик безопасности и без изменения существующей инфраструктуры.

Расширенная техническая поддержка

Поставка решения сопровождается услугами расширенной технической поддержки со стороны специалистов «Лаборатории Касперского» (в рамках соглашения о сервисном обслуживании, Maintenance Service Agreement). Профессиональная помощь доступна в круглосуточном режиме 24x7. Время реакции на инцидент или запрос составляет не более 30 минут. Помимо этого с вами будет работать персональный технический менеджер, хорошо знакомый с потребностями вашего бизнеса.