



Локальная репутационная
база, повышающая
безопасность изолированных
сетей

Kaspersky Private Security Network

kaspersky АКТИВИРУЙ
БУДУЩЕЕ



Kaspersky Private Security Network

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
- Поставщики управляемых услуг безопасности и другие сервис-провайдеры

Преимущества для бизнеса

- Оптимизация обнаружения вредоносных объектов
- 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
- Создание собственной базы вердиктов
- Соблюдение нормативных требований по обеспечению безопасности изолированных систем и сред

Репутационная база данных об угрозах для изолированных сетей

Сложные и целевые атаки наносят куда более серьезный ущерб, чем массовое вредоносное ПО. В условиях растущего количества угроз нельзя недооценивать значимость аналитики, которую в режиме реального времени предоставляет облачная служба Kaspersky Security Network. **Kaspersky Private Security Network** (KPSN) – это локальная копия облачной базы данных. При использовании этой службы ни один бит данных о найденных угрозах не уйдет из сети предприятия наружу, даже в центры обработки данных «Лаборатории Касперского», что никак не отразится на доступности глобальной облачной базы знаний.

Преимущества Kaspersky Private Security Network



Сведения о новейших и наиболее сложных атаках, предоставляемые в реальном времени в рамках контролируемой среды вашей локальной сети



Полная совместимость с нормативными и законодательными требованиями и стандартами безопасности



Интеграция со сторонними приложениями через протокол HTTP



Высокая доступность и кластеризация



Высокий уровень обнаружения угроз и низкий уровень ложноположительных срабатываний – визитная карточка защитных решений «Лаборатории Касперского»



Облачная аналитика без необходимости передачи данных за пределы организации



Адаптация решения к условиям полной изоляции сети по методу «воздушного зазора» (air gap)



Гибкие возможности развертывания

Высокий уровень безопасности для изолированных сетей

Требования к облачным технологиям безопасности критичных и изолированных сетей постоянно растут, и для соответствия им большинство решений использует «кеширующие прокси-серверы» – ограниченную выборку данных или заранее определенные необновляемые репутационные базы данных. Решение Kaspersky Private Security Network отличается от них тем, что оно может полностью обеспечивать **безопасность с использованием облачных технологий локально**, внутри принадлежащих организации центров обработки данных, не передавая на сторонние серверы никакой информации.

Принцип работы

Kaspersky Private Security Network устанавливается на стороне заказчика, и у штатных IT-специалистов остается полный контроль над безопасностью корпоративных данных. Ваш центр анализа событий ИБ сможет воспользоваться преимуществами облачной базы данных без риска для конфиденциальности и с соблюдением нормативных требований, не допускающих передачи данных за периметр корпоративной сети.



Служба проверки репутации **файлов**

Эта служба предоставляет установленным у вас решениям «Лаборатории Касперского» информацию о репутации и категориях файлов.

Защита от целевых и APT-угроз

Платформа Kaspersky Anti Targeted Attack предоставляет решению Kaspersky Private Security Network репутационные данные IP-адресов и доменных имен с целью максимально быстрого обнаружения целевых атак и передовых угроз.

Антиспам

Антиспам предоставляет данные статистики для защиты от спама.

Служба проверки репутации

URL-адресов

Эта служба предоставляет информацию о репутации и категориях веб-сайтов.

Системные требования

Для установки Kaspersky Private Security Network требуется выделенный сервер со следующими характеристиками:



Аппаратные требования

16-ядерный процессор, 2.8 ГГц
96 ГБ оперативной памяти (RAM)
2 ТБ свободного места на твердотельном накопителе (SSD)



Программные требования

Ubuntu 20.04 LTS
Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7.1)
Astra Linux Special Edition РУСБ.10015-01 (оперативные обновления 1.7.3 и 1.7.3-uu2)
Astra Linux Special Edition РУСБ.10015-16 исп. 1 (оперативное обновление 1.7.3)
Astra Linux Special Edition РУСБ.10015-01 (оперативное обновление 1.7.4)
Браузеры: Google Chrome, Mozilla Firefox, Microsoft Edge

Прочие конфигурации развертывания приведены в руководстве для администраторов.

Лицензирование



**Kaspersky
Private Security
Network**
Standard

Поддержка до 50 000 защищаемых устройств



**Kaspersky
Private Security
Network**
Advanced

Поддержка до 500 000 защищаемых устройств

Локальная репутационная база данных
(собственные черные и белые списки компании)

Поддержка модели xSP

Высокая доступность

Данные об угрозах – важная и неотъемлемая часть стратегии защиты. Kaspersky Private Security Network позволяет усилить уровень безопасности вашей компании без риска передачи данных за пределы корпоративной сети.



Kaspersky Private Security Network

[Подробнее](#)

www.kaspersky.ru

© 2023 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)