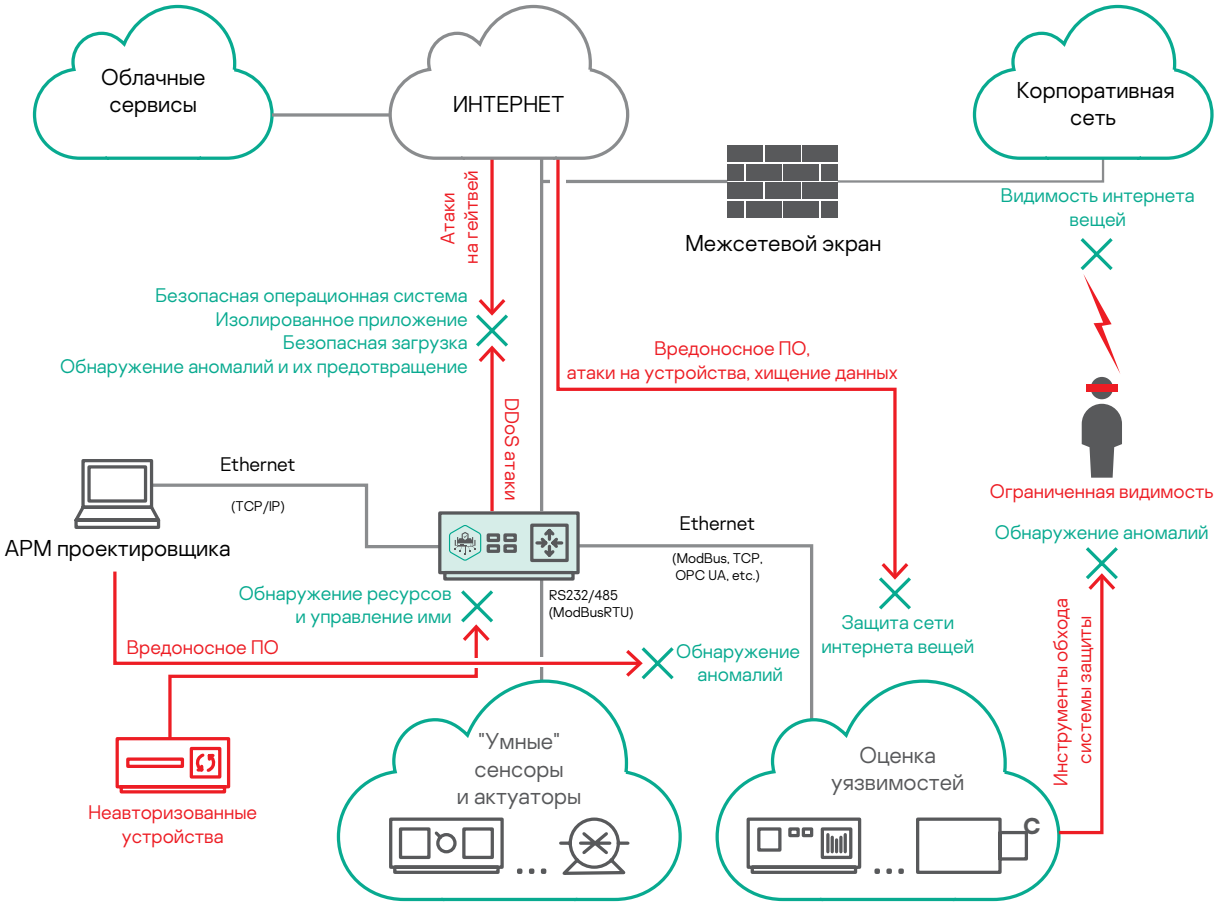
kaspersky

Kaspersky
IoT Secure Gateway

Kaspersky IoT Secure Gateway β*

Одно из центральных и наиболее важных устройств в IoT-сети и в то же время наиболее уязвимое к угрозам безопасности - гейтвей. Подключение к внешним сетям, достаточные вычислительные ресурсы и зачастую прошивка на базе устаревшей версии ОС делают его мишенью для атак и внедрения вредоносного ПО. Поэтому именно гейтвей в первую очередь нуждается в надежной защите.

Kaspersky IoT Secure Gateway – это решение, предназначенное для построения безопасных систем интернета вещей. Предлагаемое нами решение является настраиваемым и может дополнятся функционалом, уже имеющимся в продуктах партнеров, заинтересованных в сотрудничестве.



* Продукт предназначен для некоммерческого пилотирования

Возможности и преимущества

Подключение

Ethernet	
Маршрутизация и NAT	
DHCP-сервер	
MQTT-брокер	MQTT-брокер на базе Mosquitto позволяет осуществлять сбор данных и управление подключенными IoT-устройствами (сенсорами и актуаторами, умными реле и т. п.).
OpenSSL/TLS	
MQTT поверх TLS	Позволяет осуществлять безопасное подключение и защищенную передачу данных между гейтвеем и облачной платформой.
Интеграция с облачными сервисами	AWS, Azure, Mindsphere, IBM Watson и т.д.

Мониторинг

Обнаружение и классификация устройств	Обнаруживает и категоризирует IoT-устройства на основе их сетевой активности. В пользовательском интерфейсе можно увидеть все подключенные к сети устройства. Новое устройство будет обнаружено при подключении к сети в течение 60 секунд.
Отчеты и уведомления (MQTT, SYSLOG, Push-уведомления)	При обнаружении нового подключенного к сети устройства администратору будет отправлено соответствующее уведомление.

Гибкое управление защитой и шлюзом

Веб-интерфейс	
Push-уведомления	
Система централизованного управления и мониторинга (Kaspersky Security Center)	Централизованное управление реализуется посредством подключения гейтвеев к серверу Kaspersky Security Center, который коррелирует события безопасности, полученные со всех подключенных устройств, происходит управление из одной точки всеми продуктами Kaspersky на всех устройствах сети.

Защита IoT-шлюза от кибератак

KasperskyOS	В основе KasperskyOS лежит надежное микроядро, которое допускает только определенный способ взаимодействия. Будучи компактным, оно может использоваться на различных платформах. Защитный компонент Kaspersky Security System контролирует взаимодействие между всеми частями системы, делая эксплуатацию уязвимостей бесполезной для злоумышленников. Архитектура приложений основана на компонентной модели, благодаря чему разработка решения становится проще и удобнее.
Безопасная загрузка	Безопасная загрузка осуществляет верификацию целостности и подлинности прошивки с использованием криптографических методов на IoT-устройствах перед загрузкой образа. Несанкционированно измененная или поврежденная прошивка не будет загружена. Безопасная загрузка может использоваться совместно с аппаратным хранилищем ключей.
Безопасное обновление	Технология Безопасного обновления работает в комплексе с Безопасной загрузкой и позволяет обновлять прошивку только с использованием правильно подписанных и зашифрованных образов из доверенных источников. Безопасное обновление работает следующим образом: · С консоли управления поступает команда на скачивание. · Загрузчик обновления получает образ обновления. · Загрузчик сохраняет образ во временное хранилище обновлений и запечатывает его. · Данные из хранилища передаются на проверку специальному контроллеру. · Этот контроллер выполняет проверку образа и авторизует его в случае успеха. · Авторизованный образ поступает в апдейтер.

Безопасный аудит	Безопасный аудит – это функция KasperskyOS, которая распознает, записывает и сохраняет журнал аудита, предоставляя гарантии того, что записи журнала не будут подменены. Ключевые свойства: • Аудируемые события определяются независимо на пользовательском и системном уровне и регулируются политиками под управлением Kaspersky Security System. • Источник аудируемых событий, признанный KasperskyOS надежным, добавляется в журнал аудита. • Безопасный аудит располагает гибкой и масштабируемой архитектурой хранилища журнала аудита. • Предусмотрена схема обнаружения подмены журнала аудита. • Безопасный аудит соответствует требованиям ISO/IEC 15408-2.

Защита IoT-инфраструктуры

IPS/IDS и сетевой экран	Для защиты от сетевых атак используются два разных механизма, дополняющих друг друга: межсетевое экранирование и обнаружение вредоносной активности на базе сигнатурного анализа (IPS\IDS) трафика. Межсетевое экранирование обеспечивает защиту от несанкционированного сетевого доступа, а обнаружение вредоносной активности позволяет своевременно заблокировать атаку на узлы защищаемой сети.
Корень доверия (Root of trust)	Этот подход базируется на цепочке доверия (chain of trust). Начальная точка доверия выбирается в зависимости от требуемых гарантий, и в самых сложных случаях устанавливается на уровне аппаратной части.
Репутационный сервис Kaspersky Security Network (reputation service)	Kaspersky Security Network (KSN) – это комплексная распределенная инфраструктура, которая предназначена для обработки данных о киберинцидентах, которые поступают от миллионов пользователей со всего мира, давших свое согласие на передачу такой информации. Облачная система KSN доставляет эти ценные сведения на каждое устройство. KSN позволяет обеспечить высочайший уровень защиты и максимальную скорость реакции на угрозы при минимальном уровне ложноположительных срабатываний.
Сканер устройств интернета вещей и база уязвимостей (IoT Monitor & VulnDB)	Сканер устройств интернета вещей и база уязвимостей – это технология, предназначенная для обнаружения всех устройств интернета вещей (контроллеры, IP-камеры, HMI др.) в сети пользователя. После обнаружения устройств решение проверяет их на наличие уязвимостей, которые могут эксплуатировать злоумышленники. Если уязвимости найдены, сканер предлагает рекомендации по их устранению и повышению уровня безопасности.

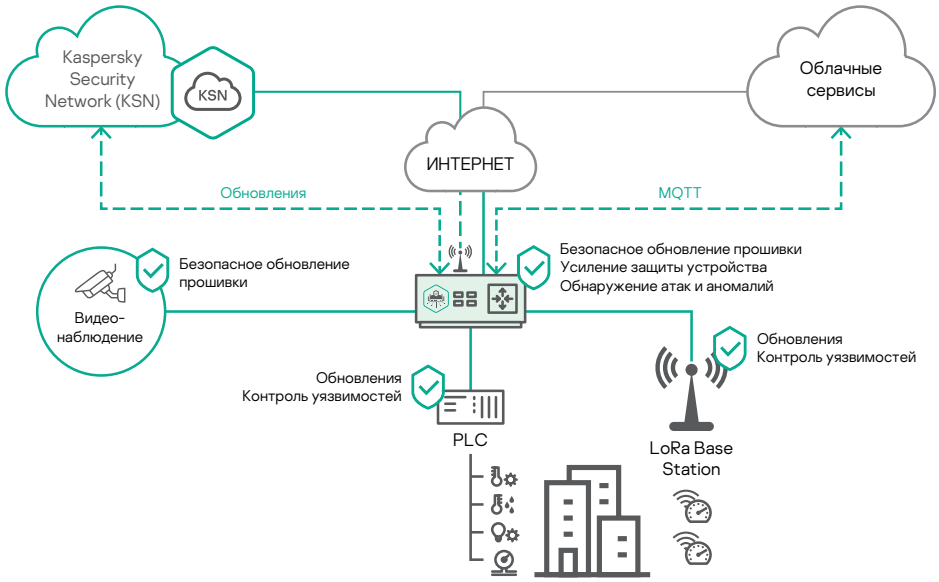
Спецификация поддерживаемого аппаратного обеспечения (Advantech UTX-3117)

Processor System	Intel Apollo Lake E3900 & N series Processor, 2MB L2 Cache
Memory	Dual channel DDR3L 1867MHz, up to 8GB
Graphics	Intel Apollo Lake E3900 Series SoC Intel Apollo Lake N series SoC Interface HDMI: 1, max resolution up to 3840 x 2160 @ 30Hz DP1.2: 1, max resolution up to 4096 x 2160 @ 60Hz
Ethernet	Dual 10/100/1000Mbps LAN LAN1: Intel I210AT LAN2: Realtek RTL8111G
I/O Interface	1 x RS-232 with 5v/12v 1 x RS-422/485 full duplex with Phoenix connector 2 x USB3.0 port 1 x SATA interface, support SSD TPM Infineon SLB9665 chip onboard. Support TPM2.0
Storage	1 x SATA II SSD bay mSATA 1, co-lay with H/S miniPCIE slot
Expansion	1 x Half-Size Mini PCIe support Sub1G module (i.e.: Zigbee) or mSATA 1 x Full-Size Mini PCIe support 3G/LTE module with SIM holder 1 x M.2 E key support Wi-Fi module

Примеры реализаций

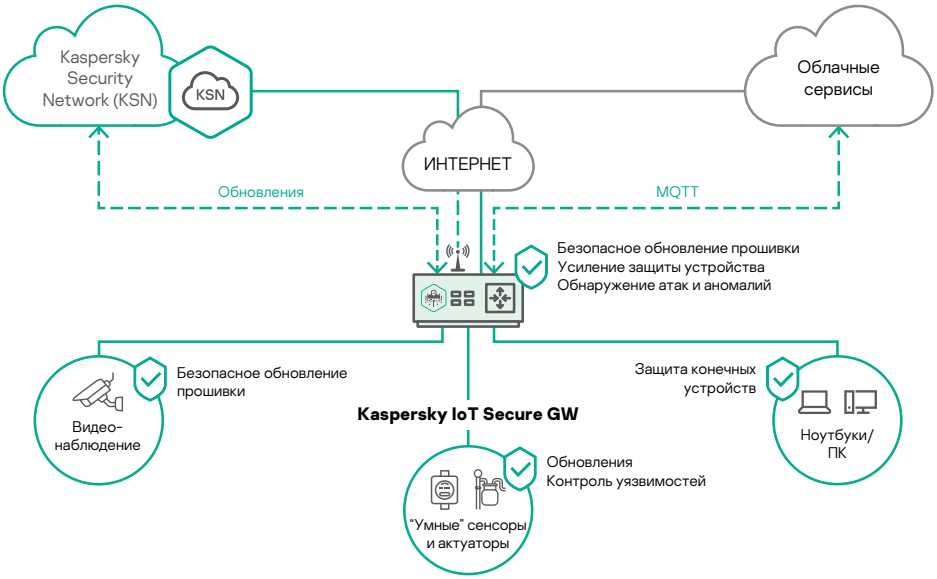
Умный город на основе Kaspersky IoT Secure Gateway

В доме устанавливаются системы контроля потребления ресурсов, системы управления электричеством и водоснабжением. Внутриквартирные счетчики подключаются по беспроводному протоколу LoRaWAN. Системы видеонаблюдения с удаленным доступом, датчики движения и датчики открытия дверей отвечают за физическую безопасность, а информационную безопасность обеспечивают технологии Kaspersky IoT Secure Gateway, которые блокируют атаки на локальные устройства и рабочие станции, выявляют неавторизованное подключение к сети и защищают периметр сети и связь с облаком.



Умный склад на основе Kaspersky IoT Secure Gateway

На складе устанавливаются системы контроля климатических параметров с возможностью управления из облака, что позволяет непрерывно поддерживать и контролировать климат на складе из любой точки. Использование RFID-датчиков и меток позволяет вести автоматизированный складской учет, который контролируется как локально с рабочих мест пользователей в сети, так и централизованно. Системы видеонаблюдения с удаленным доступом и датчики объема и открытия дверей отвечают за физическую безопасность, а информационную безопасность обеспечивают технологии Kaspersky IoT Secure Gateway, которые блокируют атаки на локальные рабочие станции, выявляют неавторизованное подключение к сети и защищают периметр сети и связь с облаком.



Kaspersky IoT Secure Gateway

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru