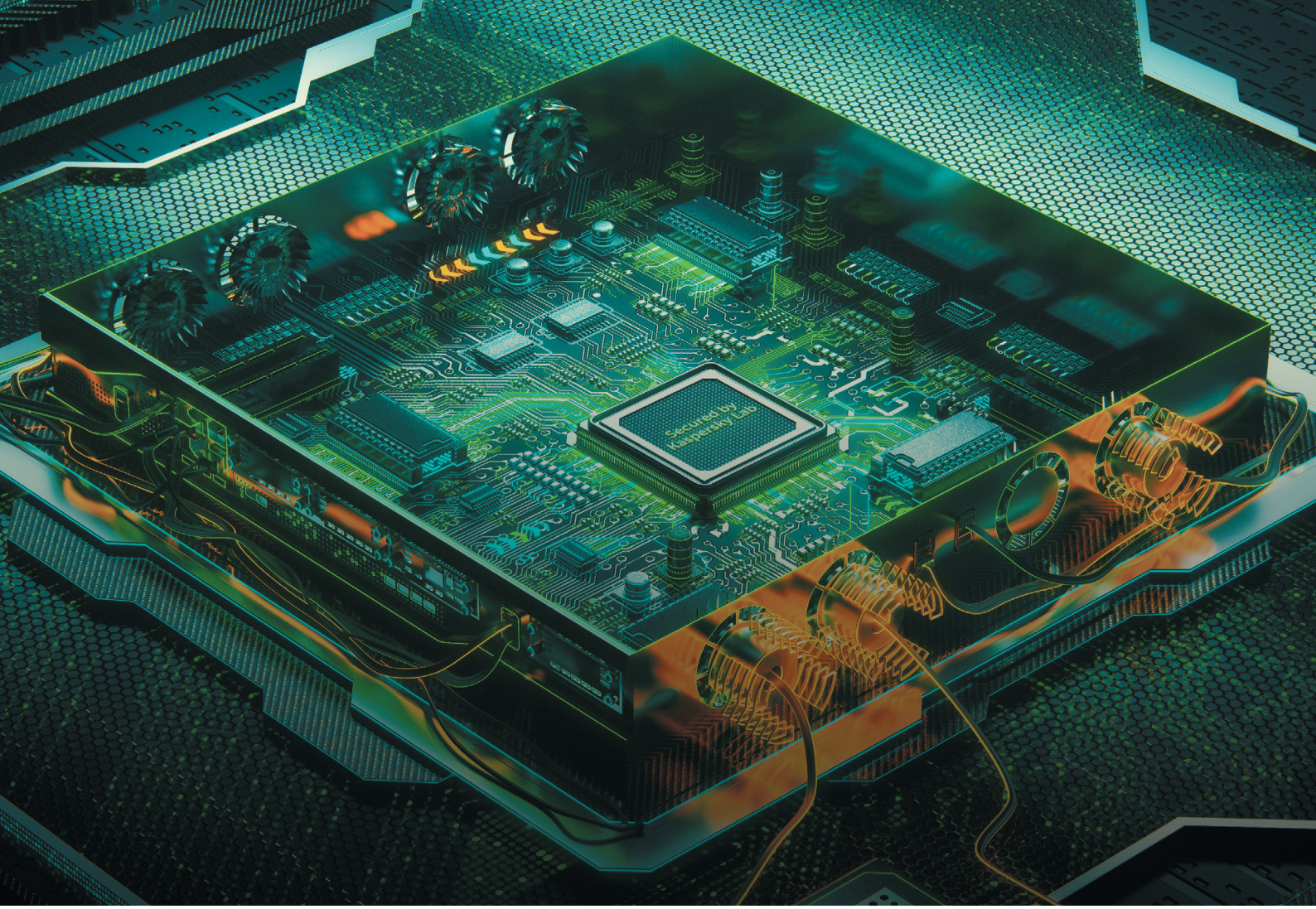

Безопасная ОС для интернета вещей

kaspersky АКТИВИРУЙ БУДУЩЕЕ

KasperskyOS®

KasperskyOS®

KasperskyOS – операционная система, позволяющая обеспечить безопасную эксплуатацию ПО, в том числе небезопасных приложений.

KasperskyOS также обеспечивает защиту при случайных ошибках ПО и неправомерных действиях пользователей.

Общая информация

Интернет вещей меняет мир прямо на наших глазах. Он может сделать его безопаснее, улучшить состояние здоровья людей, помочь экономить время и деньги, уменьшить расходы и добавить новое измерение в управление производством и в жизнь в целом.

Концепция интернета вещей охватывает огромное количество устройств, приспособлений, технологий, программного обеспечения и протоколов передачи данных. Такая неоднородная среда подвержена большому количеству рисков безопасности, которые могут представлять угрозу для различных сторон нашей жизни, связанных с интернетом вещей.

Наша цель – получить максимум возможных преимуществ интернета вещей, при этом сведя к минимуму сопутствующие риски.

Основой большинства устройств интернета вещей являются операционные системы общего назначения, которые не могут соответствовать предъявляемым к ним специфическим требованиям безопасности. Эти системы, как правило, отличаются повышенной функциональностью, что не является обязательным для подключенных устройств. В то же время, исправлению многочисленных уязвимостей, вызванных слабой архитектурой, плохой реализацией и ненадлежащим использованием операционных систем в этих устройствах, практически не уделяется внимания.

Два основных типа устройств интернета вещей, которые подвергаются атакам:

33,6% Роутер

23,2% DVR (цифровая видеокамера)

Глубокая интеграция устройств интернета вещей в нашу повседневную жизнь означает, что их безопасность имеет первостепенное значение. Так как подключённых устройств много, применение дополнительных элементов управления безопасностью каждого устройства является бесполезным и нецелесообразным. Безопасность должна быть встроенной, она должна соответствовать требованиям окружающей среды и поддерживать функциональность системы без каких-либо ограничений.

Ключевой элемент безопасности интернета вещей, который можно предусмотреть заранее, – это правильные политики безопасности. Ввиду разнообразия устройств интернета вещей:

- механизмы применения политик безопасности должны быть максимально адаптивными (насколько возможно);
- определение политик безопасности должно быть простым и понятным, но при этом достаточно выразительным для того, чтобы создавать правила без ошибок и упущений;
- политики не должны ослаблять существующие меры безопасности, препятствовать функционалу системы в работе или значительно снижать производительность системы, приложения или самого устройства.

62% пользователей в случае атаки обвинят в потере данных компанию, допустившую утечку

77% организаций по всему миру как минимум один раз стали жертвой кибератаки в 2017 г.

Основой большинства устройств интернета вещей являются операционные системы общего назначения, которые не могут соответствовать предъявляемым к ним специфическим требованиям безопасности.

Цели

Чтобы решить вопросы кибербезопасности интернета вещей и при этом минимизировать время, необходимое для разработки защитных средств, мы предлагаем KasperskyOS – операционную систему, позволяющую обеспечить безопасную эксплуатацию ПО, в том числе небезопасных приложений. KasperskyOS также обеспечивает защиту при случайных ошибках ПО и неправомерных действиях пользователей.

Особенности

Одним из наиболее важных компонентов KasperskyOS является Kaspersky Security System (KSS) – гибкий безопасный движок, который позволяет определить и применить политики безопасности для устройств интернета вещей.

Kaspersky Security System основан на принципе изоляции безопасных компонентов от функциональных в рамках одной информационной системы. Такой подход гарантирует безопасную работу системы независимо от того, каким образом реализованы функциональные компоненты, и позволяет создавать доверенные системы с использованием недоверенных компонентов. В результате политики безопасности могут быть изменены без внесения каких-либо изменений в функциональные компоненты. KSS поддерживает комбинацию различных моделей безопасности, включая возможность одновременного использования базовых и специализированных политик.

KSS – это больше, чем защита от вредоносных программ: он также предотвращает нарушение правил безопасности. Наше решение позволяет сделать систему защищённой, не снижая при этом её надёжность. Kaspersky Security System встраивается в прошивку устройств интернета вещей, выполняя вычисление вердиктов безопасности, которые определяются и преднастраиваются производителем.

Безопасное обновление

Одним из наиболее важных сервисов для интернета вещей является сервис безопасного обновления аппаратного обеспечения устройства. Kaspersky Secure Updater – это технология, которая обеспечивает два важных элемента безопасного обновления ПО. Во-первых, она гарантирует, что обновление не скомпрометировано и не было изменено в процессе передачи. Это реализуется с помощью различных криптографических методов. Во-вторых, компонент, выполняющий процесс обновления, минимально использует доверенный код, что позволяет значительно сократить поверхность атаки. Безопасность большой части апдейтера не настолько важна, так как если эти части кода скомпрометированы, злоумышленник всё равно не сможет обойти апдейтер и механизмы защиты безопасного обновления, чтобы внедрить в прошивку вредоносный код.

Безопасное хранилище

Безопасное хранилище – это база данных «ключ-значение» с простым интерфейсом, подходящим для хранения важных конфигурационных параметров. Каждый параметр в базе данных соотносится со своими атрибутами безопасности.

Политика безопасности может быть применена для установки/получения определенного параметра на основе его атрибутов безопасности. Также можно установить политику безопасности для всех настроек обновлений, которые отвечают за то, чтобы обновления индивидуальных параметров были согласованы друг с другом.

KSS использует безопасное хранилище для хранения параметров политик безопасности. Хранилище также может использоваться любым приложением в системе. Политика безопасности определяет, к каким параметрам имеет доступ каждое приложение.

Технические требования

- Требования к CPU: Memory Management Unit (MMU); IOMMU (SDMA для ARM) настоятельно рекомендуется для надежной изоляции аппаратных ресурсов;
- Поддерживаемая архитектура: x86, x86_64, ARMv5, ARMv7, ARMv8 и MIPS32;
- Протестированные аппаратные платформы: Intel Generic и Atom CPUs, NXP i.MX6 (Solo, Duo и Quad), NXP i. MX27, TI Sitara AM335x, TI Sitara AM43xx, HiSilicon Kirin620, MIPS24k.
- Минимальный объём RAM зависит от решения. Рекомендуемый объём RAM 128 Мб.

Патенты

Технологии, составляющие основу KasperskyOS и Kaspersky Security System, имеют ряд патентов:

US 7386885 B1, US 7730535 B1,
US 8370918 B1, EP 2575318 A1,
US 8522008 B2, US 20130333018 A1,
US 8381282 B1, EP 2575317 A1,
US 8370922 B1, EP 2575319 A1,
US 9015797 B1, DE 202014104595 U1.

Безопасный аудит

Ещё один важный элемент – технология Безопасного аудита, предлагаемая «Лабораторией Касперского». Она использует механизмы блокчейна и позволяет сохранять события, связанные с безопасностью, в специальном хранилище, гарантируя целостность и подлинность этих записей. Если запись фальсифицирована, оператор сможет однозначно сказать, до какого момента журнал является достоверным, и когда в него были внесены изменения.

Количество атак на устройства интернета вещей в 2017 г. выросло на 600% и достигло 50 000

Преимущества

Исходная безопасность. KasperskyOS – это безопасно спроектированная операционная система, и мы намерены и дальше поддерживать её безопасность, используя лучшие практики разработки программного обеспечения.

Универсальная модульная архитектура. Создание системы на основе слабосвязанных модулей помогает свести к минимуму объём доверенного кода и адаптировать каждое решение к индивидуальным потребностям клиента.

Грамотно спроектированные приложения. Компонентный подход к созданию безопасных приложений делает их разработку более простой и удобной, что помогает сократить время, необходимое для вывода новых продуктов на рынок.

Гибкая конфигурация безопасности. Продуманные инструменты настройки упрощают создание декларативных правил и их комбинаций для управления взаимодействиями в системе.

Отделение функций приложений от функций безопасности. Архитектура системы спроектирована таким образом, чтобы отделить функции безопасности от бизнес-логики приложений. Это упрощает настройку политик безопасности и разработку приложений.

Полноценная защита для подключенных устройств. KasperskyOS – это надёжная платформа для встроенных систем, которые имеют особые требования к кибербезопасности.

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru