kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Embedded System Security

Комплексная защита для встраиваемых систем

Встраиваемые системы давно и прочно проникли в нашу повседневную жизнь. Они повсюду: от платежных терминалов и банкоматов до медицинских устройств и автоматизированных АЗС. По мере того как растет рынок встраиваемых систем, киберпреступники приспосабливают свои тактики, методы и процедуры к атакам на новые устройства. Появляются новые схемы мошенничества, например модель «Вредоносное ПО как услуга» (MaaS), при использовании которой требования к наличию у злоумышленников специальных знаний сильно снижаются. При этом значительная часть встраиваемых систем до сих пор базируется на ОС Windows XP, поддержка которой прекращена производителем. Наличие старых, уязвимых к угрозам ОС облегчает задачу для злоумышленников.

Kaspersky Embedded Systems Security – это комплексное решение, разработанное специально для защиты встраиваемых систем. Оно включает защиту от вредоносного ПО и эксплойтов в режиме реального времени с использованием глобальной репутационной базы, а также содержит гибкие возможности управления и обеспечивает высокий уровень безопасности для устаревших систем, которые больше не поддерживаются большинством поставщиков защитных решений.

Основные проблемы в области безопасности

Хотя встраиваемые системы во многом схожи с обычными компьютерами, их эксплуатация связана с рядом специфических сложностей. Некоторые свойственны всем встраиваемым системам, другие характерны лишь для некоторых типов. Вот некоторые из типичных проблем:

Устаревшее, уязвимое программное обеспечение. Чем дольше эксплуатируется оборудование, тем выше риск того, что прекратится поддержка операционной системы и приложений, которые оно использует. Неисправленными уязвимостями могут воспользоваться преступники.

Нерегулярная установка обновлений безопасности. Даже если поставщик поддерживает ПО, исправления не всегда устанавливаются своевременно. Это может быть связано со сложностью обновления ПО на географически распределенных устройствах или с необходимостью отключения устройств от сети для установки обновлений, а также с задержками из-за тестирования обновлений перед их развертыванием в производственной среде.

Непрерывность процессов. Обновление может требовать временного вывода оборудования из эксплуатации. Для некоторых типов устройств, например медицинских, это крайне нежелательно, поэтому исправления часто устанавливаются несвоевременно.

Размещение устройств в общественных местах. Многие встраиваемые системы расположены в общественных местах, что повышает риск атаки. Сетевая защита неэффективна в случае физического заражения устройства.

Повышенные риски, связанные с контекстом использования. Многие встраиваемые системы используются для выполнения финансовых операций и (или) обработки конфиденциальной информации и кажутся киберпреступникам особенно привлекательными.

Строгие нормативные требования. Поскольку встраиваемые системы используются для обработки финансовой информации и персональных данных, на многие из них распространяются более строгие требования к обеспечению безопасности.

Внутренние угрозы. Согласно данным «Лаборатории Касперского», более 50% успешных атак на встраиваемые системы проходят при участии инсайдеров – сотрудников компании или сторонних поставщиков услуг.

Ключевые преимущества

Эффективная защита встраиваемых систем

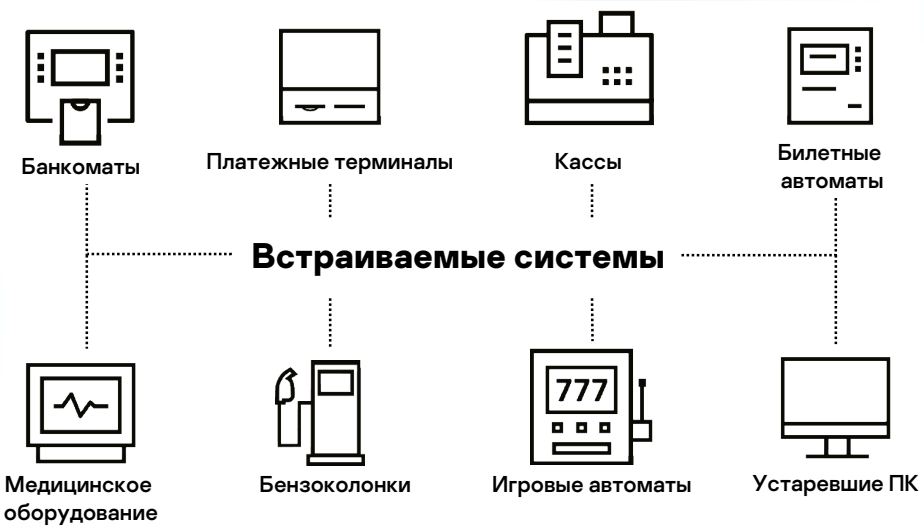
Kaspersky Embedded Systems Security – это надежное комплексное решение, которое предлагает несколько уровней защиты для устройств разной мощности с разными сценариями развертывания программного обеспечения.

Современная защита для устаревших систем

Решение Kaspersky Embedded Systems Security оптимизировано для работы на разных операционных системах – от Windows XP до новейшей Windows 11. Мы планируем продолжать поддержку Windows XP в обозримом будущем, чтобы клиенты могли постепенно обновить оборудование в удобном для них темпе.

Высокий уровень защиты при ограниченных ресурсах

Kaspersky Embedded Systems Security эффективно работает даже на низкопроизводительном оборудовании.



Основные возможности

Дополнительная защита от вредоносного ПО

На дополнительном уровне защиты, который можно развернуть в локальной или облачной среде, используется точная логика обнаружения известных, неизвестных и продвинутых угроз на основе локальных или облачных аналитических данных об угрозах, методов эвристического анализа и моделей машинного обучения.

Защита от эксплойтов

Решение защищает от эксплуатации уязвимостей приложений и системных компонентов, что позволяет противостоять более продвинутым атакам, а также защищает от бесфайловых угроз и от тех, которые обходят средства контроля программ, работающих в режиме «Запрет по умолчанию».

Инструменты контроля

Инструменты контроля приложений, устройств и обновлений допускают использование только доверенных приложений, периферийных устройств и источников обновлений, что еще больше укрепляет защиту вашей системы. Они блокируют загрузку и запуск программ, использование которых на вашем устройстве не предусмотрено, включая вредоносное ПО и приложения, которыми могут воспользоваться злоумышленники.

Защита от сетевых угроз

Решение предотвращает любые вторжения в операционную систему, защищая от сканирования портов, атак путем подбора пароля и эксплуатации уязвимостей сети. Таким образом вы можете заблокировать некоторые из основных векторов атаки на встраиваемые системы.

Контроль целостности и соблюдение нормативных требований*

Инструмент контроля целостности файлов и доступа к реестру отслеживает действия с отдельными разделами реестра, файлами и папками и может блокировать нежелательные изменения. С его помощью можно обнаружить не только атаки вредоносных программ, но и попытки прямого доступа к критически важным ресурсам или их изменения в локальном режиме. Такие меры противодействия часто рекомендуются в регламентах по защите данных, поэтому их принятие способствует соблюдению требований.

Поддержка маломощных и устаревших систем

Решение эффективно работает даже на низкопроизводительном оборудовании и поддерживает оборудование с устаревшим ОС, вплоть до Windows XP SP2. Вы можете пользоваться старыми моделями устройств, пока их обновление не станет целесообразным.

Анализ журналов*

Контроль целостности защищаемой среды осуществляется на основе анализа записей в журнале событий Windows. Приложение уведомляет администратора, если обнаруживает аномальное поведение, которое может свидетельствовать о попытке кибератаки.

Локальное и облачное управление

В зависимости от потребностей вашего бизнеса, управление корпоративными встраиваемыми системами может осуществляться через локальный сервер управления или облачную SaaS-консоль. Локальное управление подойдет для тех компаний, которым важно обеспечить высокий уровень конфиденциальности данных, а облачное управление позволяет сократить как капитальные, так и операционные затраты, оперативно повысить безопасность рабочих процессов и снизить нагрузку на IT-администраторов.

Управление сетевым экраном

Сетевой экран Windows можно настроить непосредственно из Kaspersky Security Center, что позволяет с удобством управлять локальным сетевым экраном из единой консоли. Эта функция особенно полезна, если встраиваемые системы находятся не в домене и параметры сетевого экрана Windows нельзя настроить централизованно.

*Только в расширенной лицензии Kaspersky Embedded Systems Security Compliance Edition

Связаться с нами

Нужна дополнительная информация?
Свяжитесь с нами прямо сейчас!

Купить у партнера

Решили приобрести решение?
Найдите партнера в своем регионе!

www.kaspersky.ru