

Kaspersky Embedded Systems Security

Комплексная защита для встраиваемых систем

Встраиваемые системы прочно вошли 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 техники, тактики и процедуры для атак на подобные устройства.

Главные вызовы для безопасности встраиваемых систем

Устаревшее уязвимое ПО

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



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.



Размещение в общественных местах

Многие встраиваемые устройства расположены в общественных местах, что существенно повышает риск атаки Сетевая защита неэффективна в случае физического заражения устройства



Привлекательность для злоумышленников

Встраиваемые системы часто используются для выполнения финансовых операций и обработки конфиденциальной информации, поэтому кажутся киберпреступникам особенно привлекательными.



Строгие нормативные требования

Поскольку встраиваемые системы используются для обработки финансовой информации и персональных данных, на многие из них распространяются 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 поставшиков



Распространение встраиваемых систем на базе Linux

Встраиваемые системы на базе Linux быстро набирают популярность, в том числе среди киберпреступников. При этом выбор специализированных защитных решений для Linux куда более ограничен, чем для Windows.

Ландшафт угроз

По разным причинам миллионы встраиваемых систем и компьютеров все еще работают под управлением устаревших уязвимых ОС. Несмотря на прекращение поддержки многих версий Windows, они используются до сих пор: большинство встраиваемых устройств работает под управлением Windows XP. Для злоумышленников это приглашение к действию.

Тем временем появляется все больше встраиваемых систем на базе Linux, и киберпреступники не только адаптируют к этим системам свои методы, но и изобретают новые инструменты для атаки. Система Linux считается защищенной по умолчанию, однако полагаться на эту мнимую защищенность крайне опасно. Несмотря на то что злоумышленники до сих пор не проявляли к этой ОС большого интереса, они активно наверстывают упущенное. При этом выбор защитных решений для встраиваемых систем на базе Linux куда более ограничен, чем для устройств с Windows.

По данным «Лаборатории Касперского», количество атак на банкоматы и платежные терминалы существенно выросло в 2022 году: оно на 19% превысило показатель 2020 года и на 4% – показатель 2021 года и продолжает расти.

Kaspersky Embedded Systems Security – это комплексное решение, разработанное специально для защиты встраиваемых систем. Оно предоставляет защиту от вредоносного ПО и эксплойтов, и гибкие возможности контроля и управления, обеспечивая максимально возможный уровень безопасности для встраиваемых устройств на базе операционных систем Windows и Linux.

Атаки на физическом уровне

- Атаки методом «черного ящика»
- Замена панели для ввода ПИН-кода / использование скиммеров
- Скрытые камеры
- Взрывы

Атаки на уровне программного обеспечения

- Удаленная/ локальная установка вредоносного ПО
- Анализаторы памяти (снифферы) / атаки на ОС
- Заражение/изменение связующего ПО

Атаки на уровне сети

- Уязвимости VPN-подключения
- Брутфорс-атаки по протоколу RDP
- · RCE-эксплойты
- Удаленная установка

Более половины успешных атак на встраиваемые системы проходят при участии инсайдеров – сотрудников компании или сторонних поставщиков услуг.



Ключевые преимущества

Оптимальная защита встраиваемых систем

Kaspersky Embedded Systems Security предлагает несколько уровней защиты для устройств разной мощности и предусматривает разные сценарии развертывания. Решение совместимо с операционными системами Windows и Linux.

Защита устаревших и современных систем

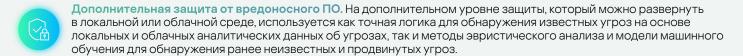
Решение оптимизировано для работы на разных операционных системах – от Windows XP до Windows 11. Мы планируем продолжать поддержку Windows XP в обозримом будущем, чтобы клиенты могли обновить оборудование в удобном для них темпе. Kaspersky Embedded Systems Security также поддерживает новейшие архитектуры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

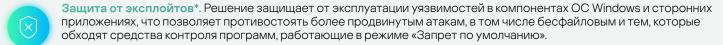
Высокая степень защиты даже для маломощных систем

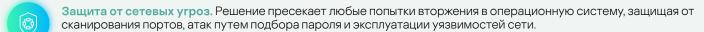
Kaspersky Embedded Systems Security эффективно работает даже на низкопроизводительном оборудовании.

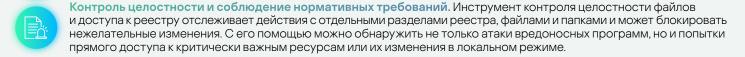
Основные возможности

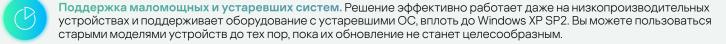


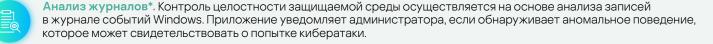


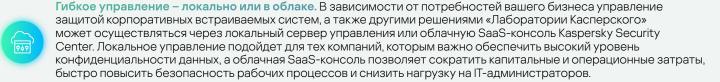












Управление сетевым экраном. Можно настроить встроенный в ОС сетевой экран непосредственно из Kaspersky Security Center и в дальнейшем с удобством управлять им из единой консоли. Эта функция особенно полезна, если встраиваемые системы находятся не в домене и параметры сетевого экрана Windows/Linux нельзя настроить централизованно.

Эффективная защита даже при нестабильном подключении к сети. Проблема нестабильности сетевого подключения характерна для многих встраиваемых систем, расположенных в удаленных зонах с низким качеством сотовой связи, вблизи источников радиосигналов и так далее. Peшение Kaspersky Embedded Systems Security эффективно даже при слабом сигнале и полном отсутствии сетевого подключения.





Профессиональные сервисы и расширенная техническая поддержка

Надлежащее обслуживание защитных решений на протяжении их жизненного цикла – процесс трудоемкий, а обеспечение безопасности встраиваемых систем, которые существенно отличаются от обычных рабочих станций, – еще более сложная задача. Но у нас есть удобное решение – Профессиональные сервисы «Лаборатории Касперского». Мы возьмем на себя все задачи по обслуживанию защитного решения на каждом этапе его жизненного цикла – от развертывания, обновления, настройки и оптимизации производительности до миграции на новое оборудование. В рамках Расширенной технической поддержки вам будет помогать персональный менеджер по техническим вопросам, а наши опытные эксперты будут обрабатывать инциденты в вашей инфраструктуре в приоритетном порядке.

Связанные продукты и сервисы



Каspersky Threat Intelligence. Широкий набор сервисов, который объединяет аналитические данные об угрозах из разных источников, потоки данных об угрозах и результаты собственных исследований и позволяет вам получить полное представление об опасностях, которые могут угрожать вашей организации.



Анализ защищенности платежных систем. Всесторонний анализ защищенности банкоматов и платежных терминалов, формирующий четкое представление о текущем уровне защищенности ваших систем, на основе которого вы можете принять дополнительные меры безопасности, оптимизировать защитное решение и устранить уязвимости в системе безопасности.



Kaspersky Security для бизнеса.

Передовые технологии, которые используются во всем мире для защиты рабочих мест, серверов, рабочих станций и мобильных устройств. Простое управление с помощью единой консоли.

Где актуальна защита встраиваемых систем

Отрасли

ि

Финансовый сектор

Транспорт и туризм (продажа билетов)

靊

Розничная торговля

Ресторанный и гостиничный бизнес

础

Здравоохранение

圃

Государственный и некоммерческий сектор

虚

Развлечения

Устройства



Банкоматы



Билетные автоматы



Бензоколонки



Кассы



Платежные терминалы



Медицинское оборудование



Устаревшие компьютеры



Игровые автоматы

Подробнее о продукте