

Kaspersky Embedded Systems Security

kaspersky

Главные вызовы для безопасности встраиваемых систем

1. **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.
2. **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.
3. **Размещение в общественных местах.** Многие встраиваемые устройства расположены в общественных местах, что существенно повышает риск атаки. Сетевая защита неэффективна в случае физического заражения устройства.
4. **Привлекательность для злоумышленников.** Встраиваемые системы часто используются для выполнения финансовых операций и обработки конфиденциальной информации, поэтому кажутся киберпреступникам особенно привлекательными.
5. **Строгие нормативные требования.** Поскольку встраиваемые системы используются для обработки финансовой информации и персональных данных, на многие из них распространяются строгие требования к обеспечению безопасности.
6. **Внутренние угрозы.** Согласно данным «Лаборатории Касперского», более 50% успешных атак на встраиваемые системы проходят при участии инсайдеров – сотрудников компании или сторонних поставщиков услуг.
7. **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.

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.

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.

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.

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 и, в случае последнего, может работать как на x86 так и на ARM-системах.

Высокая степень защиты даже для маломощных систем

Kaspersky Embedded Systems Security эффективно работает даже на низкопроизводительном оборудовании.

Основные возможности

Укрепление системы (контроль безопасности). Средства управления приложениями, устройствами и обновлениями допускают использование только доверенных приложений, периферийных устройств и источников обновлений, что еще больше укрепляет защиту вашей системы. Они блокируют несанкционированную загрузку и запуск программ, в том числе вредоносного ПО и приложений, которыми могут воспользоваться злоумышленники.

Дополнительная защита от вредоносного ПО. На дополнительном уровне защиты, который можно развернуть в локальной или облачной среде, используется как точная логика для обнаружения известных угроз на основе локальных и облачных аналитических данных об угрозах, так и методы эвристического анализа и модели машинного обучения для обнаружения ранее неизвестных и продвинутых угроз. Специализированная технология защиты от шифрования обеспечивает вашим устройствам надежную защиту от программ-вымогателей.

Защита от эксплойтов*. Решение защищает от эксплуатации уязвимостей в компонентах ОС Windows и сторонних приложениях, что позволяет противостоять более продвинутым атакам, в том числе бесфайловым и тем, которые обходят средства контроля программ, работающие в режиме «Запрет по умолчанию».

Защита от сетевых угроз. Решение пресекает любые попытки вторжения в операционную систему, защищая от сканирования портов, атак путем подбора пароля и эксплуатации уязвимостей сети.

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.

Поддержка маломощных и устаревших систем*. Решение эффективно работает даже на низкопроизводительных устройствах и поддерживает оборудование с устаревшими ОС, вплоть до Windows XP SP2. Вы можете пользоваться старыми моделями устройств до тех пор, 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.

Гибкое управление – локально или в облаке. В зависимости от потребностей вашего бизнеса управление защитой корпоративных встраиваемых систем, а также другими решениями «Лаборатории Касперского» может осуществляться через локальный сервер управления или облачную SaaS-консоль Kaspersky Security Center. Локальное управление подойдет для тех компаний, которым важно обеспечить высокий уровень конфиденциальности данных, а облачная SaaS-консоль позволяет сократить капитальные и операционные затраты, быстро повысить безопасность рабочих процессов и снизить нагрузку на IT-администраторов.

Управление шифрованием данных*: Одна консоль для полнодискового шифрования — защита от офлайн-вмешательства, управляемость в любых условиях.

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. Решение Kaspersky Embedded Systems Security эффективно даже при слабом сигнале и полном отсутствии сетевого подключения.

Интеграция с MDR. Решение интегрируется с SOC «Лаборатории Касперского» для круглосуточного мониторинга подозрительной активности и оперативного реагирования. Это позволяет выявлять и блокировать целевые атаки на встроенные системы на ранней стадии, предотвращая серьёзный финансовый ущерб для бизнеса.

*Только для ОС Windows

Более половины успешных атак на встроенные системы связаны с «внутренней активностью» со стороны сотрудников или сторонних сервис-провайдеров

Атаки на сетевом уровне
- Эксплуатация уязвимостей сети и VPN
- Атаки методом подбора паролей на RDP
- Удаленная установка

Удаленные программные атаки
- Удаленная установка вредоносного ПО
- Компрометация или изменения компонентов промежуточного ПО

Атаки с прямым доступом
- Установка вредоносного ПО с USB-накопителей
- Прямое вмешательство в ОС и промежуточное ПО

Внутренние угрозы
- Локальное подразделение
- Сервисная компания
- Злоупотребление легитимными инструментами и правами доступа

Прямые кибератаки
- Прямое заражение
- Офлайн-манипуляции (с выключением устройства)
- Атаки с использованием BadUSB

Физические атаки
- Поддельные PIN-пады и скиммеры
- Скрытые камеры
- Blackbox-атаки на диспенсер
- Физическое разрушение — взрывы, саботаж и т.д.



Компрометация через сеть
- Из офисной сети — компрометация сотрудника с последующим латеральным перемещением
- Неавторизованные подключенные устройства (использование LAN-розеток в офисе, скомпрометированные точки доступа Wi-Fi)
- Поддельные базовые станции сотовой связи

Обратная инфекция
- Компрометация при прямом контакте
- Применяется для дальнейшего доступа к офисной сети

Цепочка поставок
- Уже заражено при доставке
- Специализированное ПО, скомпрометированное на этапах разработки или сборки ПАК

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



Kaspersky 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)
- Розничная торговля
- Ресторанный и гостиничный бизнес
- Здравоохранение
- Государственный и некоммерческий сектор
- Развлечения

Устройства

- Банкоматы
- Билетные автоматы
- Бензоколонки
- Кассы
- Платежные терминалы
- Медицинское оборудование
- Устаревшие компьютеры
- Игровые автоматы

www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее