Kaspersky® Embedded Systems Security

Комплексная защита для встраиваемых систем

Рынок встраиваемых систем постоянно растет. Для киберпреступников он тоже становится все более и более привлекательным. В 2018 году вредоносное ПО, предназначенное для банкоматов и POS-систем, поразило на 142% больше целей, чем в 2017 году.

Встраиваемые системы давно и прочно проникли в нашу повседневную жизнь. Они повсюду: от POS-терминалов и банкоматов до медицинских и телекоммуникационных устройств. Это значит, что количество векторов атаки также значительно возросло.

Киберпреступники все чаще переключают внимание на встраиваемые системы, стремясь использовать их как точку проникновения в корпоративную сеть. Теперь у компаний нет другого выхода, как организовывать более продуманную защиту систем и данных. Kaspersky Embedded Systems Security – это комплексное решение, разработанное специально для защиты встраиваемых систем. Оно включает защиту от вредоносного ПО в реальном времени с использованием глобальной репутационной базы, контроль приложений и устройств, а также содержит гибкие возможности управления.

Основные преимущества

Эффективная работа даже на низкопроизводительном оборудовании

Kaspersky Embedded Systems Security эффективно работает даже на низкопроизводительном оборудовании. Архитектура решения обеспечивает надежную защиту без перегрузки системы. Минимальные системные требования – всего 256 МБ оперативной памяти для семейства Windows XP и 50 МБ свободного места на жестком диске (в режиме «Запрет по умолчанию»).

Оптимизировано для работы с Windows XP

Большая часть встраиваемых систем до сих пор базируется на ОС Windows XP, поддержка которой прекращена производителем. Решение Kaspersky Embedded Systems Security оптимизировано для работы на операционных системах – от Windows XP до Windows 10. Мы не планируем прекращать поддержку Windows XP в обозримом будущем, так что у вас будет достаточно времени, чтобы обновить оборудование.

Защита памяти

Мощная технология защиты от эксплойтов отслеживает критически важные процессы и предотвращает эксплуатацию уязвимостей приложений и системных компонентов, в том числе угрозы «нулевого дня». Это особенно важно для защиты от широко распространенных программ-вымогателей, таких как WannaCry и ExPetr.

Соблюдение требований

Уникальный комплексный набор компонентов защиты в Kaspersky Embedded Systems Security (антивирус , контроль устройств и приложений, управление сетевым экраном, мониторинг целостности файлов и аудит журналов событий) обнаруживает и блокирует вредоносные действия против вашей системы, а также выявляет различные индикаторы нарушения безопасности – в соответствии с нормативными требованиями (включая PCI/DSS, SWIFT и т. д.).

Возможности

Мощная защита от вредоносного ПО

Сочетание проактивных облачных методов обнаружения и анализа с традиционными технологиями обеспечивает защиту от известных, новых и сложных угроз. Антивирус является опциональным, но крайне рекомендуемым модулем классической защиты. Отключение его возможно для сценариев с использованием низкопроизводительного оборудования или медленных каналов связи.

Облачная защита

Kaspersky Security Network – это глобальная облачная сеть «Лаборатории Касперского». Миллионы узлов по всему миру непрерывно поставляют аналитические данные в наши системы, что позволяет защитным продуктам быстро реагировать даже на самые новые угрозы, в том числе на массовые атаки. Постоянный поток новых данных о попытках вредоносных атак и подозрительном поведении позволяет мгновенно выносить заключения о каждом файле, таким образом обеспечивая постоянную защиту от новейших угроз.

Контроль программ

Применение сценария «Запрет по умолчанию» с технологией контроля запуска программ оптимизирует устойчивость вашей системы к атакам. Запретив выполнение любых приложений, кроме доверенных программ, служб и надежных системных компонентов, можно автоматически заблокировать большинство видов вредоносных программ. Контроль распространения программного обеспечения реализует подход «доверенных установщиков»: больше не нужно долго и утомительно вручную переносить в белый список файлы, созданные или измененные во время обновления или установки ПО. Просто пометьте установщик как доверенный, и процедура обновления пройдет как обычно.

Мониторинг и контроль устройств

Технология контроля устройств позволяет следить за USB-накопителями, физически подключенными или пытающимися подключиться к аппаратному оборудованию. Закрытие неавторизованным устройствам хранения доступа к системе блокирует одну из основных для киберпреступников «точек входа», которыми они пользуются для проведения вредоносных атак. Все подключения USB-устройств отслеживаются и сохраняются в журнале, поэтому ненадлежащее использование USB может быть определено как возможный источник атаки в процессе расследования инцидента и реагирования на него.

Управление сетевым экраном Windows

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 централизованно настроить.

Контроль целостности файлов*

Контроль целостности файлов отслеживает действия с выбранными файлами и папками. Вы также можете настроить отслеживание изменений в файлах, произошедшие тогда, когда мониторинг был прерван.

Аудит записей журнала*

Kaspersky Embedded Systems Security следит за целостностью защищаемой среды на основе записей в журнале событий Windows. Приложение уведомляет администратора, если обнаруживает аномальное поведение, которое может свидетельствовать о попытке кибератаки.

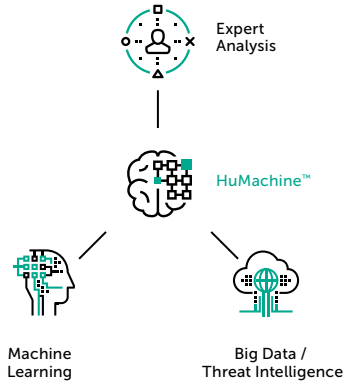
Интеграция с SIEM-системами

Kaspersky Embedded Systems Security умеет передавать события из журнала приложений по протоколу syslog. Это значит, что они могут быть перенесены и успешно обработаны в SIEM-системе. События можно напрямую экспортировать из Kaspersky Embedded System Security в SIEM или централизованно через Kaspersky Security Center.

Гибкое управление

Решением можно локально управлять из командной строки, графического интерфейса или централизованно на основе политик Kaspersky Security Center. Политики безопасности, обновления сигнатур, антивирусные проверки и сбор результатов – все это легко контролировать из единой консоли управления. Кроме того, всеми объектами в локальной сети можно управлять через любую локальную консоль: это особенно важно при использовании изолированных или сегментированных сетей, что является обычным сценарием использования встраиваемых систем.

* Доступно в версии Kaspersky Embedded Systems Security Compliance Edition.



www.kaspersky.ru