Kaspersky Embedded Systems Security

Комплексная защита для встраиваемых систем

Количество киберугроз, угрожающих критически важным бизнес-процессам, постоянно растет. Все чаще объектом атаки становятся встраиваемые системы, которые встречаются повсюду — например в банкоматах, киосках самообслуживания, POS-системах, медицинском оборудовании, автоматах по продаже билетов.

Защитить встраиваемые системы особенно трудно: часто они распределены географически и редко обновляются. При этом они должны быть устойчивыми к отказам и сбоям, поскольку обрабатывают наличность и данные банковских карт. А еще, помимо защиты самих устройств, нужно не допустить их использования как точек входа в корпоративную сеть при атаках извне или с участием инсайдеров.

Стандартные требования к безопасности встраиваемых систем, как правило, предусматривают лишь борьбу с вирусами и усиление защиты. Этого недостаточно. Требуется новый подход: прежде всего нужно применять технологии контроля устройств и запрета по умолчанию и при необходимости дополнять их антивирусом.

Преимущества решения

Низкие требования к аппаратным ресурсам

Архитектура решения позволяет ему эффективно работать даже на низкопроизводительном оборудовании: Kaspersky Embedded Systems Security обеспечивает надежную защиту, не перегружая систему.

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 полного сохранения функциональности при работе на платформе Windows XP, а также на устройствах под управлением Windows 7, Windows 2009 и Windows 10.

В отличие от других поставщиков защитных решений, которые отказываются от поддержки Windows XP, решение Kaspersky Embedded Systems Security в обозримом будущем будет поддерживать эту операционную систему.

Сценарий «Запрет по умолчанию»

Последние годы растет количество вредоносного ПО, созданного специально для атак на встраиваемые системы (примеры таких атак — Tyupkin, Skimer, Carbanak). Большинство традиционных антивирусных решений не обеспечивают полной защиты от таких сложных целенаправленных угроз. При использовании сценария «Запрет по умолчанию» в системе исполняются только те файлы, драйверы и библиотеки, которые явно разрешены администратором.

Контроль устройств

Инструмент 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 точек входа, которыми киберпреступники обычно пользуются для проведения вредоносных атак.

Все подключения USB-устройств отслеживаются и анализируются, поэтому ненадлежащее использование USB может быть определено как источник атаки в процессе реагирования на инцидент и его расследования.

Интеграция с SIEM-системами

Kaspersky Embedded Systems Security умеет передавать события из журнала по протоколу syslog. Это значит, что они могут перенесены и успешно обработаны в SIEM-системе.

Защита памяти

Решение защищает процессы в памяти от эксплойтов. Динамически загружаемый агент встраивается в защищаемые процессы, следит за их целостностью и снижает риск использования уязвимостей.

Централизованное управление

Политики безопасности, обновления сигнатур, расписание проверок и просмотр отчетов — все это доступно в единой консоли Kaspersky Security Center. Всеми средствами защиты можно управлять через любую локальную консоль: это особенно важно при использовании изолированных и сегментированных сетей, в которые обычно объединяются встраиваемые системы.

Профессиональная помощь

«Лаборатория Касперского» обеспечивает техническую поддержку более чем в 200 странах мира. Помощь доступна ежедневно и круглосуточно.

Специалисты компании, отвечающие за профессиональные сервисы, готовы помочь в любой момент, обеспечив максимальную отдачу от защитного решения «Лаборатории Касперского».

Облачная защита

«Лаборатория Касперского» рекомендует использовать для защиты аналитические данные сети Kaspersky Security Network: это позволит предотвратить атаки на основе эксплойтов, снизить возможный вред и минимизировать время реагирования.

Управление сетевым экраном и CD/DVD

Встраиваемые системы, функционирующие за пределами периметра домена, должны быть защищены как контролем устройств для CD/DVD-приводов и USB-накопителей, так и сетевым экраном. Это помогает обезопасить системы от действий инсайдеров.

Контроль целостности файлов*

Контроль целостности файлов отслеживает действия с выбранными файлами и папками. Также можно отслеживать изменения в файлах, произошедшие тогда, когда мониторинг был прерван.

Аудит записей журнала*

Kaspersky Embedded Systems Security отслеживает целостность защищаемой среды, основываясь на записях в журнале событий Windows. Администратор получает уведомление об обнаруженном нетипичном поведении системы, которое может свидетельствовать о попытке кибератаки. Решение изучает журнал событий Windows и определяет уязвимости на основе правил, созданных пользователем, на основе настроек эвристики.

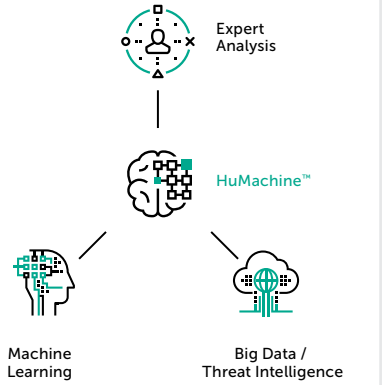
Антивирус

Антивирусный модуль предлагается в качестве дополнительного. Использование классического подхода исключительно антивирусной защиты не оправдано из-за ограничений низкопроизводительного аппаратного оборудования. Кроме того, эффективность антивируса в борьбе с новыми киберугрозами и инсайдерами крайне мала.

Режима «Запрет по умолчанию» с применением технологии контроля устройств зачастую достаточно и без антивирусного модуля, но его можно добавить в качестве дополнительного уровня безопасности.

---

* Данные функции доступны только в версии KESS Compliance Edition.



www.kaspersky.ru

#ИстиннаяБезопасность