

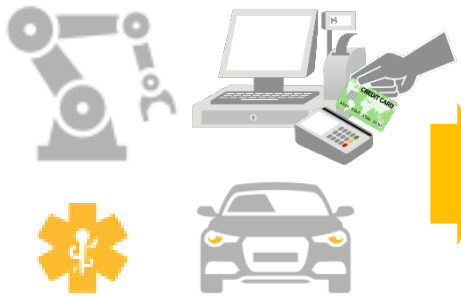


Symantec Embedded Security: Critical Systems Protection

Для каждой отрасли и компании критичные IT-активы различаются. Это могут быть промышленные системы управления, IoT-устройства, точки продаж и многое другое. Все эти системы объединяет то, что стабильность их работы очень важна для компании. Такие системы необходимо надежно защищать, при этом влияние на производительность должно быть минимальным. Развитие вычислительных сред, позволяющих получать прибыль, требуется делать «со скоростью бизнеса».



Уязвимая инфраструктура



Службы операционной системы

Службы приложений Интерактивные программы

Упрощенный вид атаки

Каждому процессу требуется ограниченный набор ресурсов и прав доступа к ним.

Но многие процессы имеют гораздо большие привилегии доступа к ресурсам, чем им требуется.

Атака «убеждает» процесс использовать имеющийся у него доступ к важным ресурсам.

Symantec Critical System Protection создан для защиты бизнес-критичных IT-активов и «Интернета вещей» (IoT), промышленных и производственных систем, финансовых и медицинских устройств.

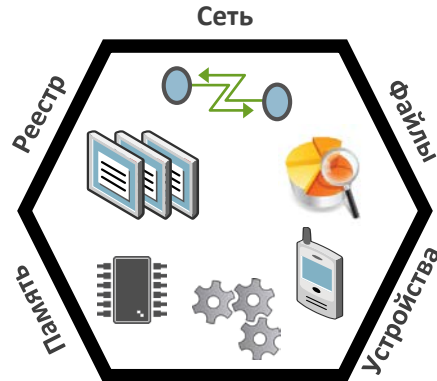
Как работает Symantec CSP

Для каждого процесса создается «песочница», которая определяет минимум привилегий для нормального доступа к ресурсам.

Это не антивирус! Ваша система всегда надежно защищена, независимо от того, известен ли уже вредоносный объект или нет.



Комплексная защита



Защита бизнеса от направленных кибератак в кратчайшие сроки



Технически проработанное зрелое решение



Обнаружение угроз в критичных IT-системах и блокировка аномальных действий



Оптимизирован для бизнес-критичных систем, высоконагруженных и маломощных устройств



Решение отлично зарекомендовало себя на крупных предприятиях различных направлений: производство, финансы, телеком и других



Symantec Embedded Security: Critical Systems Protection



Защита бизнеса от направленных кибератак в кратчайшие сроки

Встроенные возможности для упрощения и ускорения развертывания



CSP автоматически создает правила «песочницы» на основе собранных событий активности процесса во время нормального использования



Обнаружение установленных приложений для оптимизации создания политики



Решение поставляется со встроенными стратегиями безопасности, набором шаблонов политик и настройками для профилактики и выявления передовых угроз



Белый список приложений формируется с помощью нескольких щелчков мыши

Автоматизированное создание правил «песочницы»



Обнаружение угроз в критичных IT-системах

Аудит и отчетность для обеспечения соответствия политикам безопасности



Защита целостности системы и конфигурации



Аудит и мониторинг событий в системе



Аналитика событий и выявление несанкционированного доступа



Отчеты об аномальных активностях





Symantec Embedded Security: Critical Systems Protection



Технически проработанное зрелое решение

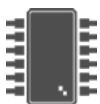
Многогранный контроль приложений и защита от целевых атак и угроз нулевого дня



Контроль входящих и исходящих сетевых подключений для каждого приложения



Блокировка установки и выполнения стороннего ПО при помощи встроенной стратегии защиты



Контроль доступа к внешним устройствам на основе пользователей и приложений



Назначение пользователей и групп, которые могут устанавливать приложения

Предотвращение исполнения стороннего ПО и модификации устройства



Белый список приложений, которые могут работать на устройстве и блокировка остальных, причем приложения из белого списка получают строго необходимые привилегии



Защита от вредоносного кода, вставленного или запущенного из памяти



Защита изменения конфигурации. Мониторинг и контроль данных приложения и конфигурации, черный список известных угроз, блокировка прямого доступа к диску



Контроль процессов, их чтения и записи в память других процессов



Оптимизирован для бизнес-критичных систем, высоконагруженных и маломощных устройств



Влияние CSP на производительность устройства минимально



Четкий контроль политик. В шаблон политики от Symantec внесите дополнения и отслеживайте изменения путем ревизий версий политик



Настройка доверенных обновлений на основе издателей, пользователей, групп, каталогов и приложений



Тонкая настройка «песочницы». Добавление исключений позволяет приложениям выполнять дополнительные действия



Защита на основе политик, поэтому в отличие от антивируса постоянного обновления сигнатур не требуется



Symantec Embedded Security: Critical Systems Protection



Решение отлично зарекомендовало себя на крупных предприятиях различных направлений: производство, финансы, телеком и других



Легко масштабировать, что очень важно для больших компаний



Центральная консоль управления для всех платформ - разработка политики, развертывание, мониторинг и отчетность



Поддержка различных версий ОС Windows, Linux и QNX.
Поддерживает широкий спектр оборудования, включая IoT-системы



Агенты могут быть развернуты в управляемых или неуправляемых режимах



Агент безопасности с возможностями, специально созданными для маломощных устройств IoT

Компактный, но очень мощный, позволяющий обеспечить комплексную защиту ИТ-систем

Принцип работы существенно отличается от антивируса, что позволяет надежно защищать

Идеально подходит для промышленных систем управления, высоконагруженных и бизнес-критичных систем

