SafenSoft

SoftControl TPSecure

Защита конечных точек банковской сети и устройств самообслуживания

О продукте

SoftControl TPSecure обеспечивает защиту электронных устройств самообслуживания (банкоматов, информационно-платежных терминалов) от несанкционированного изменения ПО и доступа к данным со стороны обслуживающего персонала или хакеров.

Использование TPSecure совместно со специальной версией **TPSecure Teller Edition** для защиты рабочих мест сотрудников фронтофиса банка (операционисты, касса) и **Enterprise Suite** для защиты рабочих станций сотрудников бэкофиса позволяет построить единую систему защиты от внешних (вредоносное ПО, хакеры) и внутренних (инсайдеры, недобросовестные сотрудники) угроз.

Принцип работы

TPSecure осуществляет контроль запуска и активности приложений, тем самым обеспечивает целостность ПО в процессе работы и сохранение системы в последнем заведомо исправном состоянии. Благодаря этому, TPSecure надежно защищает систему от всех видов вредоносного ПО и несанкционированного доступа к данным без необходимости обновлений.

TPSecure Unattended Device

Оптимально подходит для защиты устройств самообслуживания использующих как низко-, так и высокоскоростные каналы связи. Для развертывания и изменения политик контроля TPSecure могут применяться как собственная система централизованного управления, так и Microsoft SCCM, HP OpenView, IBM Tivoli и другие средства управления ИТ-инфраструктурой.

TPSecure Teller

Эффективен для защиты рабочих станций с установленным специализированным ПО (клиент АБС, АСР и др.), позволяет осуществлять мониторинг и логирование действий сотрудника наряду с сохранением целостности системы и защитой от несанкционированных изменений.

TPSecure iBanking

Предназначен для обеспечения безопасного интернет-банкинга, защищая компьютер от внедрения вредоносного кода, нелегитимных модификаций и изменений настроек клиента ДБО. Предлагая TPSecure iBanking своим клиентам, банк минимизирует риск взлома компьютера клиента и осуществления злоумышленниками операций в системе ДБО.

Защита специализированного ПО

В TPSecure возможна гибкая настройка пользовательских правил как для отдельных приложений, так и для их групп. Это позволяет TPSecure интегрироваться со специализированным ПО (например, с АСР банкомата) для контроля его целостности, защиты от изменения программного кода, защиты хранимых локально данных, включая временные файлы приложений.

Возможности и преимущества

Защита от несанкционированного доступа к данным и изменения ПО	
Динамический контроль целостности	Осуществляется контроль запуска приложений, запуск новых приложений может быть автоматически заблокирован или приостановлен до получения подтверждения от администратора.
Динамическая песочница	Запуск неизвестных или потенциально уязвимых приложений TPSecure осуществляет в безопасной изолированной среде - "песочнице", поэтому они не могут влиять на другие процессы или нанести вред системе.
Контроль активности приложений	TPSecure контролирует доступ различных приложений к файловой системе, ключам реестра, внешним устройствам и сетевым ресурсам. Возможно создание пользовательских правил активности приложений.
Специализированные функции для защиты УС	
Различные варианты установки	Кроме стандартной и централизованной установки, есть возможность установки в тихом режиме (через командную строку), а также клонирования предварительно настроенной программы с эталонного УС.
Отключение централизованного управления	Для УС, имеющих низкоскоростное подключение к сети, возможно отключение централизованного управления клиентскими модулями TPSecure. Это сведет к нулю трафик TPSecure при неизменном уровне защиты.
Доступ к внешним устройствам	Возможна гибкая настройка правил доступа к внешним USB, CD/DVD носителям, отключение автозапуска и настройка исключений (по типу устройства, имени, производителю, ID). Кроме того, возможна блокировка всех CD/DVD носителей кроме защищенных, а также настройка правил доступа к COM, LPT портам.
Скрытый мониторинг и логирование	Операции по доступу и копированию данных, включая копирование на внешние устройства, отслеживаются и логируются с возможностью получения уведомлений.
Система самозащиты	Никто, кроме авторизованных администраторов, не может подключиться, остановить или удалить клиентское приложение, даже с правами локального администратора.
Специализированные функции для защиты рабочих станций банка	
Контроль запуска приложений	Возможно заблокировать запуск сотрудником всех новых приложений либо только определённых приложений.
Запись текста, введенного с клавиатуры	Позволяет узнать, какие данные и в каком приложении сотрудник вводил с клавиатуры.
Откат изменений	Сохранение истории изменений для определённого приложения позволяет откатить изменения файлов, отредактированных с помощью этого приложения.
Система учета рабочего времени сотрудника (общего и с каждым приложением)	Позволяет осуществлять мониторинг и создавать отчёты о времени работы сотрудника с тем или иным приложением, а также суммарное время работы на рабочей станции.
Совместимость с другими решениями	Возможность совместной работы с установленным ПО и другими средствами защиты (любые средства защиты каналов передачи данных, почты и шифрования, большинство антивирусов).
Обработка инцидентов и получение уведомлений	Консоль администрирования позволяет удалённо принимать решения о блокировке или запуске новых приложений, изменять настройки. А также получать уведомления о статусе защиты при доступе, изменении, удалении файлов и ключей реестра, за которыми ведётся наблюдение.
Централизованное администрирование	
Помогает выполнить требования PCI DSS и ЦБ РФ	SoftControl TPSecure поможет компании привести систему в соответствие стандарту PCI DSS и снизить финансовые риски и риски ИБ.
Гибкость решения и индивидуальный подход	
Различные варианты поставки	Возможна поставка как стандартного набора компонент и настроек, так и разработка дополнительного функционала по требованию заказчика. Возможна поставка исходного кода продукта, двоичных библиотек (SDK).

Выгода использования

Комплексная защита от внешних и внутренних угроз

Защита без необходимости регулярных обновлений

Поможет привести систему в соответствие требованиям стандартов PCI DSS и ЦБ РФ

Простота интеграции с другими системами защиты

Индивидуальный подход и возможность реализации дополнительного функционала на заказ

Различные варианты поставки, включая исходный код и двоичные библиотеки (SDK)

Поддерживаемые платформы

Устройства самообслуживания

Поддерживаются все популярные платформы под управлением Microsoft Windows Embedded.

Рабочие станции

Операционные системы: Windows XP Embedded, Windows XP, Windows Embedded POSReady 2009, Windows Embedded Standard 7 , Windows Embedded POSReady 7, Windows 7, Windows Embedded 8.1 Industry Pro, Windows Embedded 8.0 Standard, Windows 8, Windows 8.1, Windows 10 Enterprise.

Дисковое пространство: 150 МБ

Интеграция со сторонними средствами управления ИТ-инфраструктурой

Возможность использования API для управления продуктом.

О компании Safe`n`Sec Corporation

Safe`n`Sec Corporation основана в 2008 году. Основным направлением деятельности компании является разработка программных продуктов, обеспечивающих высокий уровень информационной безопасности для банкоматов, платёжных терминалов, компьютеров сотрудников банков и других финансовых организаций. Эксперты компании принимают активное участие в разработке стандартов таких международных организаций как PCI Security Standards Council и ATMIA.

В настоящий момент клиентами Safe`n`Sec Corporation являются крупнейшие российские банки, а также финансовые организации из Латинской Америки, Юго-Восточной Азии и Африки.

Safe`n`Sec Corporation

127106 Россия, Москва, Алтуфьевское шоссе, 5

Телефон: +7 (495) 967-14-51

Официальный сайт: www.safensoft.com

Коммерческие вопросы: sales@safensoft.com

Техническая поддержка для корпоративных клиентов: support@safensoft.com