



SoftControl

SysContainer 6.0.55

Функциональные
характеристики

Уважаемый пользователь!

ООО «АРУДИТ СЕКЬЮРИТИ» благодарит Вас за то, что выбрали продукт SoftControl SysContainer. Специалисты компании постарались, чтобы наше программное обеспечение отвечало самым высоким требованиям в области защиты информации и в то же время было простым и удобным в работе. Мы надеемся, что SoftControl SysContainer будет Вам полезен.

АВТОРСКИЕ ПРАВА

Материалы, приведенные в настоящем документе, являются собственностью ООО «АРУДИТ СЕКЬЮРИТИ» и могут быть использованы только для личных целей приобретателя продукта. Запрещается воспроизведение отдельных частей документа, внесение правок, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения компании и ссылки на источник. Наименования и товарные знаки, приведённые в документе, являются собственностью своих законных владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Содержание данного документа может изменяться без предварительного уведомления. ООО «АРУДИТ СЕКЬЮРИТИ» не несёт ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.

ООО «АРУДИТ СЕКЬЮРИТИ», 2021 г.

Почтовый адрес:

127106, Россия, Москва

Нововладыкинский проезд, дом 8, стр. 3

ООО «АРУДИТ СЕКЬЮРИТИ»

Телефон:

+7 (499) 201-55-12

Электронная почта:

Общие вопросы и предложения: support@sns-control.ru

Коммерческие вопросы: sales@sns-control.ru

Веб-сайт компании: <http://www.sns-control.ru>

Содержание

1. Введение	4
1.1 Назначение	4
2. Требования к аппаратному и программному обеспечению	6
2.1 Системные требования SoftControl SysContainer.....	6
3. Техническая поддержка	7

1. Введение

1.1 Назначение

Инструмент SoftControl SysContainer предназначен для сокрытия содержимого системного диска компьютера в контейнере, доступ к которому прекращается, если сменилось аппаратное обеспечение компьютера. SoftControl SysContainer помогает защититься от атак, проводимых по следующим сценариям:

1. Злоумышленник похищает жесткий диск компьютера. Злоумышленник анализирует содержимое диска в лаборатории, находит уязвимости в ПО и впоследствии проводит атаку на устройства самообслуживания (банкоматы, терминалы).
2. Злоумышленник обходит защиту BIOS, загружает компьютер с внешнего носителя и анализирует содержимое жесткого диска.

При запуске процесса помещения данных в контейнер SoftControl SysContainer считывает параметры всех устройств, подключенных к компьютеру. Если при последующих запусках компьютера критических изменений в конфигурации не было обнаружено, загрузка ОС происходит на основе параметров устройств. Критическим изменением считается удаление или замена трех и более устройств. Допустима замена меньшего количества устройств*⁴.

Если имело место критическое изменение конфигурации компьютера, для загрузки ОС у пользователя запрашивается пароль, указанный им при помещении содержимого диска в контейнер.

SoftControl SysContainer является клиентским компонентом и способен работать как автономно, так и в совокупности с SoftControl Service Center. Для работы с SoftControl Service Center на компьютере с SoftControl SysContainer также должен быть установлен клиентский компонент SoftControl SysWatch, с помощью которого на SoftControl Server передаются события SoftControl SysContainer. Документ «Service Center. Руководство администратора» подробно описывает систему SoftControl Service Center.

Подробную информацию об установке, настройке и эксплуатации SoftControl SysContainer содержит документ «SoftControl SysContainer. Руководство администратора».

* Формирование ключа из подмножества устройств является криптографически надежным благодаря использованию [схемы разделения секрета Шамира](#).

SoftControl SysContainer можно применять для системных дисков компьютеров, функционирующих под управлением ОС семейства Microsoft® Windows®.

Данный продукт разработан с использованием исходных кодов VeraCrypt, лицензированных при помощи VeraCrypt License, объединяющей Apache License 2.0 и TrueCrypt License 3.0. Копия лицензии находится в папке с установленным приложением в файле *VCLicense.txt*.

2. Требования к аппаратному и программному обеспечению

2.1 Системные требования SoftControl SysContainer

Таблица 1. Минимальные системные требования

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:			
Microsoft® Windows® 7 (SP1) 64-разрядная ¹	1 ГГц	2 ГБ	100 МБ + дополнительно 10 МБ на UEFI-разделе
Microsoft® Windows® 8 32-разрядная	1 ГГц	1 ГБ	
Microsoft® Windows® 8 64-разрядная	1 ГГц	2 ГБ	
Microsoft® Windows® 8.1 32-разрядная	1 ГГц	1 ГБ	
Microsoft® Windows® 8.1 64-разрядная	1 ГГц	2 ГБ	
Microsoft® Windows® 10 32-разрядная	1 ГГц	1 ГБ	
Microsoft® Windows® 10 64-разрядная	1 ГГц	2 ГБ	
Microsoft® Windows® 10 IoT Enterprise 32-разрядная	1 ГГц	1 ГБ	
Microsoft® Windows® 10 IoT Enterprise 64-разрядная	1 ГГц	2 ГБ	
Серверные операционные системы:			
Microsoft® Windows® Server 2008 R2 64-разрядная ^{1,2}	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 64-разрядная ²	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 R2 64-разрядная ²	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2016 64-разрядная ²	1,4 ГГц	512 МБ	

Примечания:

1. Требуется обновление KB3033929 (поддержка алгоритма хэширования SHA-256 при проверке цифровой подписи) или любое его замещающее.
2. Поддерживаются только варианты установки ОС с рабочим столом.

Дополнительные требования:

- Тип BIOS должен быть UEFI. Также рекомендуется отключить опцию SecureBoot.
- Системный диск должен быть разбит в формате GPT (GUID Partition Table). В начале диска необходимо наличие нераспределенного пространства размером не менее 32 КБ.

3. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl SysContainer вы можете обращаться в техническую поддержку по электронной почте support@sns-control.ru.