SoftControl

SysWatch 6.1.398

Методика тестирования

Уважаемый пользователь!

ООО "АРУДИТ СЕКЬЮРИТИ" благодарит Вас за то, что выбрали продукт SoftControl SysWatch. 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 SysWatch будет Вам полезен.

Почтовый адрес:
127106, Россия, Москва
Нововладыкинский проезд, дом 8, стр. 3
ООО "АРУДИТ СЕКЬЮРИТИ"
Телефон:
+7 499 201-55-12
Факс:
+7 499 201-55-12
Электронная почта:
Общие вопросы и предложения: support@safensoft.com
Коммерческие вопросы: sales@safensoft.com
Веб-сайт компании: safensoft.com

Содержание

1. Введение

SoftControl SysWatch предназначен для защиты от несанкционированного доступа к информационным ресурсам устройств, функционирующих под управлением ОС семейства Microsoft® Windows®.

В данном документе приведена методика тестирования установленного продукта.

2. Подготовка стенда

Для проведения тестирования потребуются два компьютера – физических или виртуальных – с возможностью подключения USB-накопителей. Компьютеры должны быть доступны друг другу по сети. На первый компьютер («сервер») устанавливается SoftControl Service Center (см. «Руководство администратора SoftControl Service Center»). На второй компьютер (далее «клиентский компьютер») устанавливается SoftControl SysWatch (см. «Руководство пользователя SoftControl ATM Client / Endpoint Client / SClient»). На компьютере с SoftControl SysWatch собирается профиль; затем SoftControl SysWatch подключается к SoftControl Service Center.

На клиентском компьютере необходимо создать пользователей *USER1* и *USER2*, а также директории на диске *C:* со следующими именами: *No_rules*, *No_write_delete_all*, *No_write_program*, *Not_for_you*, *Not_now*. Кроме того, потребуются:

1) Два USB-накопителя (*STOR1* и *STOR2*) с произвольным содержимым.
2) Два файловых менеджера: Проводник Windows (*Explorer.exe*) и, например, *FAR.exe* (http://www.farmanager.com/download.php?l=ru). Важно, чтобы второй файловый менеджер не являлся надстройкой над Проводником Windows (*FAR.exe* удовлетворяет этому условию).
3) Два любых exe-файла, т.е. программы, не требующие установки (*PROG1* и *PROG2*).
4) Семь программ установки, т.е. файлы формата *.exe* (не *.msi*), имеющие признаки инсталлятора (см. справку ниже [5]):
   - не имеющая цифровой подписи (*INST1*);
   - имеющие действительную ЭЦП (*INST2*, *INST3*, *INST4*);
   - программа установки не самой новой версии (*INST5*) и пакет обновления для нее (*INST6*), оба с действительной ЭЦП.
   - программа установки приложения, имеющего собственный механизм обновления (например, веб-браузера), не самой новой версии (*INST7*).

Справка

Логика работы SoftControl SysWatch с инсталляторами следующая:

1. Любой исполняемый файл при запуске проверяется на наличие его хэш-суммы в профиле. Если хэш-сумма в профиле есть, файл разрешается к запуску.
2. Если хэш-суммы в профиле нет, файл проверяется на наличие признаков инсталлятора – это имя со словами *setup*, *install*, *update* или опция **Installer** в свойствах файла. Если хотя бы один признак есть, файл считается инсталлятором.
3. Если файл признан инсталлятором, SoftControl SysWatch проверяет, есть ли у него действительная электронная цифровая подпись (ЭЦП), то есть подпись, для которой в хранилище Windows на данном компьютере присутствует или ее сертификат, или какой-либо сертификат из его пути сертификации.
   a. Если подписи нет, либо ее сертификата нет в хранилище, инсталлятор признается «инсталлятором без действительной ЭЦП», и его запуск блокируется.
   b. Если у файла инсталлятора есть действительная ЭЦП, и белый список не включен, то инсталлятор разрешается к запуску.
   c. Если белый список включен, то к запуску разрешаются только инсталляторы, подписанные ЭЦП с сертификатами, присутствующими в белом списке и помеченными флажком **Доверять**.
4. Когда инсталлятор разрешается к запуску, все файлы, измененные или созданные им в системе, вносятся в профиль. Также в профиль вносится и сам файл инсталлятора, то есть повторный запуск этого файла будет разрешен независимо от признаков инсталлятора в имени или наличия сертификата его ЭЦП в белом списке.

3. Тестовые задания

Все задания выполняются либо дважды (с созданием настроек локально и в SoftControl Admin Console), либо часть из них выполняется локально, а часть – через настройки подразделения в SoftControl Service Center. Некоторые задания выполняются при помощи настроек, задаваемых в интерфейсе SoftControl SysWatch только локально. Каждое такое задание имеет пометку **Только локальные настройки**.

3.1 Контроль приложений и целостности системы

Таблица 1. Тестирование контроля приложения и целостности системы

Задание	Ожидаемый результат
Блокировка запуска неизвестных процессов	
Запустите *PROG1*.	Запуск приложения блокируется.
Запуск доверенных процессов	
Добавьте *PROG1* в профиль системы. Запустите *PROG1*.	Приложение успешно запускается.
Блокировка запуска доверенных процессов с измененным исполняемым кодом	
1) Удалите *PROG1*. Скопируйте *PROG2* в директорию с *PROG1*, измените имя исполняемого модуля *PROG2* на имя удаленного исполняемого модуля *PROG1* и запустите *PROG2*. 2) Удалите переименованный исполняемый модуль *PROG2*. Скопируйте *PROG1* в прежнюю директорию. Запустите *PROG1*.	Запуск *PROG1* после модификации кода исполняемого модуля (замены на *PROG2*) блокируется. *PROG1* успешно запускается после возврата кода к исходному состоянию. Примечание: в некоторых случаях блокировка может сохраняться до перезапуска системной службы *safensec.exe*.

3.2 Контроль программ установки

Таблица 2. Тестирование контроля программ установки

Задание	Ожидаемый результат
Блокировка запуска неподписанных программ установки	
Запустите *INST1*.	Запуск неподписанной программы установки блокируется.
Блокировка запуска программ установки с недействительной ЭЦП	
Откройте свойства файла *INST2* и убедитесь, что у	Запуск программы установки с недействительной подпи-

Задание	Ожидаемый результат
него есть действительная ЭЦП. Откройте файл *INST2* с помощью Блокнота (*Notepad.exe*), вставьте один символ, сохраните – при модификации файла ЭЦП становится недействительной. Запустите *INST2*.	сью блокируется.
Установка ПО с действительной ЭЦП	
Запустите *INST3*.	Программа установки успешно выполняет свою задачу. Установленная ею программа заносится в профиль.
Установка ПО с действительной ЭЦП и включенным белым списком сертификатов	
1) В настройках клиентского модуля установите флажок **Включить белый список сертификатов**. Сертификат ЭЦП программы установки *INST4* и все сертификаты из его пути сертификации не должны быть включены в белый список; если они там есть, необходимо снять для них флажки **Доверять**. 2) Запустите *INST4*. 3) Добавьте в белый список сертификат ЭЦП из *INST4*. 4) Запустите *INST4*.	Запуск программы установки до внесения ее сертификата ЭЦП в белый список блокируется. Приложение успешно устанавливается после внесения его сертификата ЭЦП в белый список. Примечание: следует учесть, что после добавления сертификата в белый список и запуска программы установки она будет внесена в профиль системы, и даже в случае удаления сертификата из списка она будет запускаться, так как SoftControl SysWatch будет рассматривать его как ПО из профиля системы, а не как программу установки.
Обновление ПО при помощи программы обновления с действительной ЭЦП	
1) Запустите *INST5*, установите программу. Убедитесь, что она внесена в профиль и запускается. 2) Запустите пакет обновления *INST6*. После обновления запустите обновленную программу.	Программа, установленная из *INST5*, успешно запускается после обновления.
Обновление ПО при помощи собственных механизмов	
1) Запустите *INST7*, установите программу. Убедитесь, что она внесена в профиль и запускается. 2) Запустите обновление в интерфейсе программы. После обновления запустите обновленную программу.	Программа успешно запускается после обновления.

3.3 Контроль файловой системы

Таблица 3. Тестирование контроля файловой системы

Задание	Ожидаемый результат
Работа с файловой системой без установленных ограничений, проверка работоспособности механизма политик	
1) Создайте правило файловой системы для каталога *No_rules* и вложенных объектов верхнего уровня (*C:\No_rules\#*#*), где чтение, запись и удаление разрешены. Убедитесь, что для правила выставлен флажок **Активно**. 2) Откройте каталог проводником Windows. 3) Создайте в нем новый файл. 4) Удалите только что созданный файл.	Каталог успешно открывается – операция чтения удалась. Файл успешно создан – операция записи удалась. Файл успешно удаляется – операция удаления удалась.
Работа с файловой системой с ограничениями на запись и удаление для всех приложений	
1) В каталоге *No_write_delete_all* создайте новый файл *newfile.txt*. Создайте правило для каталога *No_write_delete_all* и вложенных объектов верхнего уровня (*C:\No_write_delete_all\#*#*), где чтение разрешено, а запись и удаление запрещены. Распространите действие правила на все приложения. Убедитесь, что для правила выставлен флажок **Активно**. 2) Откройте каталог проводником Windows. 3) Попробуйте создать в нем еще один файл. 4) Попробуйте удалить файл *newfile.txt*.	Каталог успешно открывается – операция чтения удалась. Файл не создается – операция записи заблокирована. Файл не удаляется – операция удаления заблокирована.
Работа с файловой системой с ограничением на запись для определенного приложения Только локальные настройки	
1) Создайте частное правило файловой системы в свойствах приложения *FAR.exe* (или того, которое используется вместо него) для каталога *No_write_program* и вложенных объектов верхнего уровня (*C:\No_write_program\#*#*), где чтение и удаление разрешены, а запись запрещена. Убедитесь, что для правила выставлен флажок **Активно**. 2) Откройте каталог с помощью *Explorer.exe*. Создайте в нем новый файл. 3) Откройте каталог с помощью *FAR.exe*. Создайте в нем новый файл.	Каталог успешно открывается с помощью *Explorer.exe* – операция чтения удалась. Файл успешно создан с помощью *Explorer.exe* – операция записи удалась. Каталог успешно открывается с помощью *FAR.exe* – операция чтения удалась. Файл не создается с помощью *FAR.exe* – операция записи заблокирована.
Работа с файловой системой с ограничениями для определенного пользователя Только локальные настройки	

Задание	Ожидаемый результат
1) Создайте правило для каталога *Not_for_you* и вложенных объектов верхнего уровня (*C:\Not_for_you\#*#*), где чтение разрешено, а запись и удаление запрещены, для зоны доверенных приложений. Убедитесь, что для правила выставлен флажок **Активно**. В дополнительных свойствах правила распространите его действие только на пользователя *USER2*. 2) Произведите следующие действия под учетной записью пользователя *USER1*: • откройте каталог проводником Windows; • создайте в нем новый файл; • удалите только что созданный файл. 3) Произведите следующие действия под учетной записью пользователя *USER2*: • откройте каталог проводником Windows; • создайте в нем новый файл с помощью *FAR.exe*.	Каталог успешно открывается пользователем *USER1* – операция чтения удалась. Файл успешно создан пользователем *USER1* – операция записи удалась. Файл успешно удаляется пользователем *USER1* – операция удаления удалась. Каталог успешно открывается пользователем *USER2* – операция чтения удалась. Файл не создается пользователем *USER2* – операция записи заблокирована.
Работа с файловой системой с ограничениями по времени	
1) В каталоге *Not_now* создайте новый файл *newfile.txt*. Создайте правило для каталога *Not_now* и вложенных объектов верхнего уровня (*C:\Not_now\#*#*), где чтение, запись и удаление запрещены, для зоны доверенных приложений. Убедитесь, что для правила выставлен флажок **Активно**. В дополнительных свойствах правила укажите такой временной интервал, чтобы правило действовало в текущий момент, но прекращало свое действие через несколько минут. 2) Откройте каталог проводником Windows. Создайте в нем новый файл с помощью *FAR.exe*. 3) Дождитесь истечения времени действия правила. 4) Откройте каталог проводником Windows. Создайте в нем новый файл. Удалите только что созданный файл.	Каталог не открывается во время действия правила – операция чтения заблокирована. Файл не создается во время действия правила – операция записи заблокирована. Каталог успешно открывается по окончании времени действия правила – операция чтения удалась.

3.4 Контроль реестра

Для выполнения этих заданий обязательны права администратора на клиентском компьютере либо просто наличие прав на изменение реестра. Корневые разделы реестра в пути, задаваемом в правилах, должны быть указаны следующим образом:

Таблица 4. Обозначения путей в реестре

Раздел реестра	Обозначение в правилах SoftControl SysWatch
HKEY_CLASSES_ROOT	*\REGISTRY\MACHINE\SOFTWARE\CLASSES*
HKEY_LOCAL_MACHINE	*\REGISTRY\MACHINE*
HKEY_CURRENT_USER	*\REGISTRY\USER\<SID>* для пользователя с указанным идентификатором безопасности (*<SID>*)
HKEY_USERS	*\REGISTRY\USER*

Таблица 5. Тестирование контроля реестра

Задание	Ожидаемый результат
Работа с реестром с ограничениями для всех приложений	
1) Создайте ключ *HKLM\SYSTEM\Key1*. Напишите для него правило: путь *\REGISTRY\MACHINE\SYSTEM\KEY1#**#*, запись запрещена, удаление разрешено. 2) Запустите *Regedit.exe*, попробуйте создать подключ, удалить *Key1*.	Операция создания подключей заблокирована. Операция удаления *Key1* разрешена.
Работа с реестром с ограничениями для определенного пользователя Только локальные настройки	
1) Создайте ключ *HKLM\SYSTEM\Key2*. Напишите для него правило: путь *\REGISTRY\MACHINE\SYSTEM\KEY2#**#*, запись и удаление запрещены. В дополнительных свойствах правила распространите его действие только на пользователя *USER2*. Примечание: важно, чтобы *USER1* и *USER2* оба имели право запускать *Regedit.exe*, например, были администраторами. 2) Под учетной записью пользователя *USER1* запустите *Regedit.exe*. Попробуйте переименовать *Key2*, создать подключ или параметр, удалить *Key2*. 3) Произведите те же действия под учетной записью пользователя *USER2*.	Все операции для *USER1* выполнены успешно. Все операции для *USER2* блокированы.
Работа с реестром с ограничениями по времени	
1) Создайте ключ *HKLM\SYSTEM\Key3*. Напишите для него правило: путь *\REGISTRY\MACHINE\SYSTEM\KEY3#**#*, запись и удаление запрещены. В дополнительных свойствах правила укажите такой временной интервал, чтобы правило действовало в текущий момент, но прекращало свое действие через несколько минут. 2) Запустите *Regedit.exe*. Попробуйте переименовать *Key3*, создать подключ или параметр, удалить *Key3*. 3) Дождитесь истечения времени действия правила. 4) Снова запустите *Regedit.exe* и произведите те же операции.	Во время действия правила все операции заблокированы. По окончании времени действия правила все операции успешно выполняются.

3.5 Контроль съёмных носителей

Таблица 6. Тестирование контроля съемных носителей

Задание	Ожидаемый результат
Блокировка доступа ко всем USB-накопителям	
1) Установите запрет на чтение, запись и удаление для типа **USB устройства**. 2) Подключите *STOR1* к порту USB и произведите операции чтения, записи и удаления файлов с него. 3) Подключите *STOR2* к порту USB и произведите операции чтения, записи и удаления.	Все операции с файловой системой на носителях *STOR1* и *STOR2* запрещены.
Разрешение доступа к определенным USB-накопителям	
1) Подключите *STOR1* к порту USB и в дополнительных свойствах правила добавьте носитель в исключения, разрешив операции чтения, записи и удаления. Произведите операции чтения, записи и удаления файлов с носителя *STOR1*. 2) Отключите *STOR1* и подключите *STOR2* к порту USB. 3) Произведите операции чтения, записи и удаления файлов с носителя *STOR2*. 4) Отключите *STOR2* и подключите *STOR1* к порту USB. 5) Произведите операции чтения, записи и удаления файлов с носителя *STOR1*.	Все операции с файловой системой на носителе *STOR1* разрешены. Все операции с файловой системой на носителе *STOR2* запрещены.

4. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl SysWatch вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.