Технические условия развертывания ПО линейки SoftControl Syswatch (Enterprise Suite Server, Enterprise Suite, Syswatch Workstation, TPSecure Teller, TPSecure)

Назначение и состав ПО SysWatch

Программные продукты линейки SoftControl предназначены для защиты от несанкционированного доступа к информационным ресурсам рабочих станций, устройств самообслуживания и серверов, функционирующих под управлением ОС семейства Microsoft Windows.

Состав

В состав ПО SysWatch входят следующие подсистемы и функциональные модули:

- SoftControl Syswatch (клиентский модуль), который непосредственно реализует проактивную защиту на подзащитных АРМ, серверах или устройствах самообслуживания под управлением ОС MS Windows
- SoftControl Service Center (подсистема), состоящая из модулей SoftControl Server (серверный компонент), SoftControl Admin Console (консоль управления) и СУБД Microsoft SQL Server. Серверный компонент и консоль управления служат для удаленного контроля и мониторинга системы защиты техническим персоналом Заказчика.

Модуль SoftControl Syswatch:

- Устанавливается в операционную систему защищаемого устройства, Сервера или устройства самообслуживания под управлением ОС MS Windows
- Обеспечивает сбор профиля системы по окончании установки.
- Выполняет блокировку запуска недоверенных приложений.
- Выполняет блокировку запуска доверенных приложений, исполняемый код которых был модифицирован.
- Выполняет блокировку запуска программ установки, не подписанных действительным сертификатом издателя.
- Обеспечивает настройку политики контроля файловой системы по чтению, изменению, удалению каталогов и файлов, и блокировку ее нарушения.
- Обеспечивает настройку политики контроля системного реестра по изменению, удалению ключей и значений ключей реестра, и блокировку ее нарушения.
- Обеспечивает настройку политики контроля по чтению, изменению и удалению объектов файловой системы USB-устройств, в том числе задание исключений, и блокировку ее нарушения.
- Обеспечивает настройку политики контроля по доступу к CD/DVD-устройствам, LPT- и COM-портам, и блокировку ее нарушения.
- Обеспечивает настройку политики контроля сетевой активности приложений по протоколу TCP в исходящем и входящем направлении между задаваемым IP-адресом (диапазоном адресов) и портом (диапазоном портов) на защищаемом устройстве и задаваемым удаленным IP-адресом (диапазоном адресов) и портом (диапазоном портов), и блокировку ее нарушения.
- Обеспечивает самозащиту: препятствует принудительной остановке модуля, обеспечивает доступ к графическому интерфейсу и удалению модуля по паролю.
- Логирует инциденты ИБ и информацию по работе модуля в файлы текстовых отчетов.
- Поддерживает автономный режим работы и режим удаленного управления с сервера (SoftControl Server Center).

- Выполняет обновление программных модулей и антивирусных баз с управляющего сервера (SoftControl Server Center).

Подсистема SoftControl Service Center:

- Устанавливается в следующем составе: SoftControl Server, Microsoft SQL Server 2014 Express (опционально), SoftControl Admin Console. Предусмотрена возможность как совместной, так и раздельной установки модулей.
- Обеспечивает первоначальную настройку: выбор служебной базы данных, задание сетевых настроек, создание первой учетной записи.
- Обеспечивает регистрацию и авторизацию клиентских модулей.
- Отображает статус защиты УС клиентскими модулями.
- Обеспечивает запуск задач для клиентских модулей на защищаемом устройстве (сбор профиля, антивирусное сканирование, обновление).
- Обеспечивает просмотр отчетов клиентских модулей.
- Обеспечивает отправку уведомлений об инцидентах ИБ, зафиксированных клиентскими модулями, на электронную почту администратора.
- Имеет систему ретрансляции обновлений с внешних серверов и обеспечивает настройку и возможность обновления клиентских модулей с сервера (SoftControl Server).

Технические требования к установке модуля SoftControl Syswatch

- Соответствие Системным требованиям **Таблица 1.**
    - Если устройство не соответствует системным требованиям по объему оперативной памяти, то могут быть проведены подбор и тесты тонких настроек:
        - периодичность сеансов связи с Сервером управления,
        - состав логов активности доверенных процессов
- Наличие в составе ОС компоненты Filter Manager.
  Примечание: компонента присутствует в пакете обновлений SP2 для ОС MS Windows XP и в MS Windows 7. Однако наблюдались прецеденты отсутствия данной компоненты ОС в Embedded версиях ОС.
  Проверить наличие компоненты возможно следующим способом:
  В командной строке ввести
  Sc query fltmgr
  и нажать Enter
  В случае если он установлен появится сообщение о его состоянии, в противном случае – сообщение об ошибке

- Возможность проведения селфтестов как до, так и после развертывания SysWatch
- Между Сервером управления и клиентами открыта двухсторонняя связь по портам 8000 и 8088
- На устройствах отсутствует вирусное ПО.
    - Если на этапе установки клиентской компоненты на устройстве и сборе профиля встроенным антивирусным сканером будет обнаружено вирусное ПО, то потребуется удаление вирусных файлов вручную либо специальным скриптом, после чего производится повторная попытка сбора профиля системы.
    - Однако, если заражены системные файлы, то потребуется переустановка ПО устройства силами Заказчика с чистых дистрибутивов.

Таблица 1. SoftControl Syswatch. Минимальные системные требования

Операционная система	ЦП	ОЗУ	Объем свободного места на жестком диске
▪ Microsoft® Windows® XP Embedded (SP2, SP3) ▪ Microsoft® Windows® Embedded for Point of Service 1.0	800 МГц	256 МБ	150 МБ + дополнительно от 120 МБ для хранения антивирусных баз
▪ Microsoft® Windows® XP (SP2, SP3) x86 ▪ Microsoft® Windows® XP (SP2) x64 ▪ Microsoft® Windows® Server 2003 (SP2) x86/x64	800 МГц	512 МБ	
▪ Microsoft® Windows® 7 (SP1) x86/x64 ▪ Microsoft® Windows® 8 / 8.1 x86/x64 ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® Server 2016 ▪ Microsoft® Windows® Server 2019	1 ГГц	1024 МБ	

Технические условия к Аппаратно-программной среде Сервера Управления SoftControl Service Center:

- Соответствие технического обеспечения Системным Требованиям **Таблица 2**
- Установлен MS Framework 4.5
- Расположение в одной сети с клиентскими устройствами
- Открыта двухсторонняя связь с клиентскими устройствами по портам 8000 и 8088
- Открыт порт 8080 для работы с локальной или сетевой консолью управления SoftControl Service Center

Таблица 2. SoftControl Service Center. Минимальные системные требования

Операционная система	ЦП	ОЗУ	Объем свободного места на жестком диске
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® Server 2016 ▪ Microsoft® Windows® Server 2019	3 ГГц	4 ГБ	100 МБ + 417 МБ в случае установки встроенной СУБД

Технические условия к Аппаратно-программной среде Консоли Администратора SoftControl Admin Console:

- Соответствие технического обеспечения Системным Требованиям **Таблица 3**
- Установлен MS Framework 4.5
- Открыт порт 8080 для работы с Сервером Управления SoftControl Service

Таблица 3. SoftControl Admin Console. Минимальные системные требования

Операционная система	ЦП	ОЗУ	Объем свободного места на жестком диске
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® Server 2016 ▪ Microsoft® Windows® Server 2019	3 ГГц	4 ГБ	100 МБ

Возможные коллизии установки и контрмероприятия

1. **Возможные коллизии установки клиентской компоненты SysWatch**
   - при сборе профиля либо АВ сканер, либо имеющийся в компоненте Syswatch собственный анализатор определяет в системе “угрозы” (зараженный файл, неподписанный драйвер и т.д.) и сбор профиля, в случае невозможности удаления угрозы АВ сканером, не происходит.
     Контрмероприятия:
     - по отчету “THREATS” находим “угрозы” и удаляем вручную либо специальным скриптом. После чего повторяем процедуру сбора профиля.
     - Однако, если заражен системный файл - требуется, чтобы Банк перезалил банкомат с “чистых” дистрибутивов. После чего производим повторную установку SysWatch на устройство.
       Важно предусмотреть возможность оперативной «перезаливки» зараженного устройства «чистыми» дистрибутивами специалистами Банка
   - в операционной системе отсутствует компонента Filter Manager (даже при установленном XP SP2).
     Контрмероприятие:
     - производится установка данной компоненты системы Банком.
       Важно! Необходимость предварительной проверки и способ проверки наличия компоненты указана в Технических условиях к УС

2. **Возможность объективной проверки стабильности работы устройств до развертывания SysWatch и с установленным SysWatch.**
   Контрмероприятия:
   - Обеспечение присутствия на тестах специалиста компетентного в проведении селфтестов на устройствах

Данная необходимость указана в Технических условиях к защищаемому устройству

3. **Работоспособность взаимодействия клиент-сервер серверной и клиентской компоненты SysWatch на существующих каналах связи Банка**
   Контрмероприятия:
   - предварительная проверка работоспособности существующих каналов связи между Сервером Управления и защищаемым устройством по портам 8000 и 8088 (двусторонний режим обмена данными)
     Важно! Данная необходимость указана в Технических условиях к защищаемым устройством
   - подбор актуальных значений периодичности связи клиент-сервер
     Пояснение: на слабых каналах связи рекомендуется устанавливать периодичность сеансов связи клиент-сервер 300 секунд и более для возможности за это время установки шифрованного соединения и обмена данными.