StarForce Content Enterprise. Описание продукта

Версия 2.0.229.0
02.03.2023

www.star-force.com

Содержание

1 Назначение документа

Данный документ содержит описание системы StarForce Content Enterprise.

2 Глоссарий

Термин	Описание
Группа документов	Логическая сущность системы защиты, предназначенная для управления правами на защищенные документы. Права на чтение документов выдаются читателю одновременно на все документы группы. Если требуется индивидуальное управление правами на документы, то каждый такой документ должен защищаться в рамках своей индивидуальной группы документов. Группы документов организованы по принципу вложенной иерархии с одной группой верхнего уровня. Группа верхнего уровня – это корневой проект, доступ к нему есть только у администратора сайта.
Серийный номер	Уникальная строка символов, используемая в процедуре получения читателем прав на чтение документов одной группы.

3 Назначение системы

StarForce Content Enterprise – система, предназначенная для защиты документов предприятия от утечки через читателей документов. Поддерживается защита документов в формате PDF, а также в других форматах, которые можно преобразовать в PDF.

Можно также защищать ZIP-архивы с документами. В результате получается архив с защищенными документами (сохраняется внутренняя иерархия). Формат выходного архива – ZIP.

4 Функциональные характеристики

- Защита документов;
- Чтение защищенных документов;
- Контроль за чтением защищенных документов;
- Расследование утечек.

1. Защита документов

Для защиты документов используется приложение StarForce Document Protector. Его можно установить на Windows или на Linux.

1.1. При защите документов создаются защищенные файлы SFPDF. При защите архива на выходе получается архив в формате ZIP, внутри которого находятся защищенные файлы. Если среди защищаемых файлов есть неподдерживаемые форматы, можно настроить, чтобы они записывались в выходную папку в незащищенном виде либо игнорировались.

1.2. Для удобства можно сохранять профили. Файл профиля содержит параметры для защиты: группа документов и папка, в которой сохраняются защищенные документы.

1.3. Защищать документы с помощью StarForce Document Protector можно тремя способами: через интерфейс приложения, через контекстное меню Windows (щелчком правой клавиши мыши) и через командную строку. В случае использования контекстного меню необходимо выбрать профиль, чтобы защитить документ.

2. Чтение защищенных документов

Для чтения защищенных документов используется приложение StarForce Reader. Его можно установить на Windows, Linux, macOS, Android или iOS.

2.1. Интерфейс StarForce Reader поддерживает поиск по тексту, масштабирование, создание заметок

2.2. Работает защита от скриншотов.

2.3. На Windows, Linux и macOS можно печатать открытый документ из ридера при наличии соответствующего разрешения.

3. Контроль за чтением защищенных документов

Контроль осуществляется с помощью веб-сайта управления системой.

3.1. Работа с пользователями

3.1.1. На сайте есть два типа пользователей: администраторы и операторы:

3.1.1.1. У администраторов есть все права: они могут просматривать журналы, управлять пользователями, управлять группами документов и создавать новые, работать с серийными номерами и просматривать отчеты.

3.1.1.2. Операторам доступны только те группы документов, на которые их назначил один из администраторов. Они могут управлять доступными группами документов, работать с серийными номерами и просматривать отчеты и журналы.

3.1.2.Управление пользователями. Доступно только администраторам. Можно просмотреть список всех пользователей, создать нового пользователя, отредактировать или отключить существующего. При редактировании или создании пользователя его можно сделать администратором или исключить из числа администраторов.

3.2. Журналы:

3.2.1. Журнал действий пользователей содержит записи о входах в систему и выходах из системы, операциях с серийными номерами, событиях защиты документов.

3.2.2. Журнал доступа к документам содержит записи о чтении или печати защищенных документов. Можно фильтровать по серийному номеру и имени документа.

3.2.3. Журнал выдачи печатных документов содержит записи о напечатанных документах. Можно создавать новые записи и редактировать существующие.

3.3. Управление группами документов. Группа документов – это логическая сущность системы защиты, предназначенная для группировки защищаемых документов на основе прав доступа к ним. Права на чтение документов (в виде серийного номера) выдаются читателю одновременно на все документы группы.

3.3.1. Группы документов связаны друг с другом по принципу вложенной иерархии. Самая верхняя группа – root (в интерфейсе сайта она не отображается, редактировать или удалить ее нельзя). Для всех остальных групп документов есть родительская группа, в которую они вложены. Если пользователь назначен на родительскую группу документов, он автоматически получает доступ и ко всем вложенным группам. В обратную сторону это не работает.

3.3.2. Выбрав доступную группу документов, можно ее отредактировать, скопировать или удалить.

3.4. Серийные номера

3.4.1. Доступ к документам, защищенным в группе, осуществляется с помощью серийного номера. Серийный номер для одного из документов позволяет открывать все документы в группе. Также серийный номер для родительской группы документов позволяет открывать документы из вложенных групп.

3.4.2. Параметры, задаваемые для партии серийных номеров (при редактировании серийного номера отредактированные значения переопределяют значения, заданные для партии):

3.4.2.1. Основные: число серийных номеров, число активаций.

3.4.2.2. Временные: срок действия серийного номера, дата начала активаций, дата истечения серийного номера, время между активациями, срок действия активационного ключа, периодическое подтверждение лицензии.

3.4.2.3. Дополнительные: уровень привязки к компьютеру, возможности печати, работа офлайн, скрытие водяных меток, права администратора.

3.4.3. Для отдельного серийного номера можно также выбрать пользователя (тогда этот пользователь сможет открывать документы без непосредственного ввода серийного номера) и написать текстовый комментарий (параметр «Назначение»).

3.4.4. Для выбранной группы документов можно генерировать партии серийных номеров, редактировать уже сгенерированные партии или отдельные серийные номера (можно изменить все параметры, кроме числа серийных номеров в партии), также можно занести в «черный список» партию серийных номеров или отдельный серийный номер.

3.4.5. Для выбранной группы документов можно просмотреть отчет по генерациям серийных номеров, отчет по партии серийных номеров, отчет по отдельному серийному номеру и отчет по активациям в группе документов.

3.5. Водяные метки. На защищенных документах, выводимых на экран, и на печатных документах можно отображать водяные метки. Документы в каждой группе наследуют метки от родительской группы документов. Водяные метки группы root задаются в конфигурационном файле на сервере.

3.5.1. При создании новой группы документов можно отключить наследование меток, тогда метки из родительской группы не будут отображаться.

3.5.2. При создании новой группы документов можно задать для нее свои водяные метки.

4. Расследование утечек

Расследование утечек, происходящих из-за того, что кто-то фотографирует документы с экранов устройств, проводится спомощью приложения StarForce Leak Investigator. Его можно установить на Windows или на Linux. Приложение StarForce Leak Investigator позволяет по исходному документу и его скомпрометированной копии установить, на какой машине был открыт документ, когда произошла утечка.

4.1. При защите в документе выделяются особые блоки текста, сдвиги которых кодируют сведения об активации документа.

4.2. StarForce Leak Investigator позволяет наложить скомпрометированную копию на оригинал документа и произвести выравнивание, чтобы повысить точность декодирования сдвигов.

4.3. По результатам декодирования приложение выдает уникальный номер, по которому в журнале активаций можно найти сведения об активированном документе, дате и времени его последнего открытия, IP адресе и названии компьютера. Таким образом возможно локализовать утечку информации.

5 Компоненты системы

У StarForce Content Enterprise есть два варианта исполнения: On-Premises и облачная версия.

Решение StarForce Content Enterprise состоит из следующих компонентов:

1. Серверные компоненты системы, развертываемые на серверах предприятия/на серверах StarForce (в облачной версии):
   a. База данных, содержащая информацию о пользователях, группах документов, серийных номерах и активациях. В качестве СУБД используется MS SQL Server или PostgreSQL. Настройки для связи с базой данных задаются в конфигурационном файле сервера *DefaultSettings.xml*.
   b. Веб-сервис для управления системой *ProActive*. Представляет собой self-hosted-приложение, написанное на платформе ASP.NET. По умолчанию используется порт 27801. Сервис принимает запросы по HTTP/HTTPS. Адрес зависит от настроек сервиса.
   c. Веб-сайт для управления системой и активации лицензий. Работает на PHP 7.4. Запустить сайт можно в IIS или через другой подходящий веб-сервер. Связь с веб-сервисом *ProActive* происходит по HTTP/HTTPS. Модуль активации документов является частью веб-сайта и реализован в виде PHP-скрипта.
   d. Веб-сервис для защиты документов *CPS*. Защита документов осуществляется при помощи веб-сервиса ASP.NET, работающего как self-hosted-приложение. Сервис принимает запросы по HTTP/HTTPS. По умолчанию используется порт 27803. Адрес зависит от настроек сервиса.
   e. Веб-сервис для преобразования файлов разных форматов *Utility*. Преобразование файлов разных форматов в формат PDF выполняется при помощи веб-сервиса ASP.NET, работающего как self-hosted-приложение. Сервис Utility принимает запросы от сервиса *CPS* по HTTP/HTTPS. По умолчанию используется порт 27804. Адрес зависит от настроек сервиса.
2. Клиентское приложение StarForce Document Protector для защиты документов, установленное на компьютерах тех сотрудников предприятия (внутри предприятия), которым требуется защищать документы. Приложение обращается к веб-сервису *CPS* по HTTP/HTTPS.
3. Приложение StarForce Reader для просмотра защищенных документов, установленное на пользовательских устройствах читателей. Для активации лицензии документа приложение обращается к PHP-скрипту на веб-сайте. По умолчанию используется порт 80 (зависит от настроек) и относительный путь /proxy/activate.pa_proxy.
4. Приложение StarForce Leak Investigator для расследования утечек (только в версии On-Premises). Необходимые данные в приложение загружает сотрудник, выполняющий расследование.

Интегрировать StarForce Content Enterprise в систему документооборота можно при помощи API *CPS* для защиты документов. Выполнять операции, доступные через веб-сайт (например, управление серийными номерами), можно через API *ProActive*.

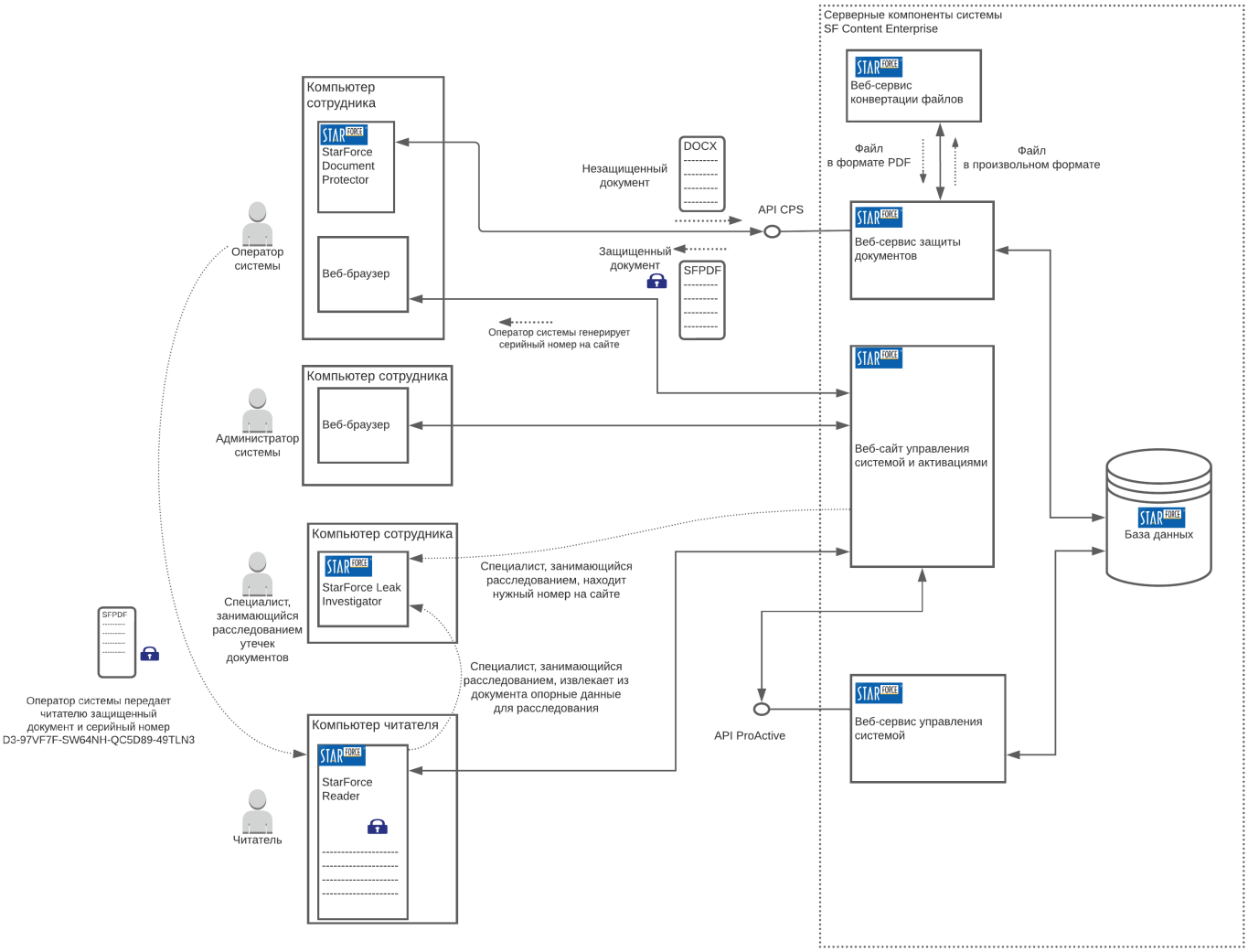

Рис. 1. Структура системы StarForce Content Enterprise

Все файлы перед защитой преобразуются в формат PDF. Пользователи могут добавлять собственные конвертеры для преобразования форматов, не поддерживаемых по умолчанию. Для этого необходимо, чтобы конвертер работал через командную строку. Конфигурационный файл сервиса *Utility* содержит примеры добавления новых средств для преобразования.

6 Требования к аппаратному и программному обеспечению

Программно-аппаратные требования для установки и корректной работы серверных компонентов системы приведены в таблице (актуальны только для версии On-Premises, подробнее в разделе Компоненты системы).

Требования	Допустимые значения
Поддерживаемые ОС	Клиентские ОС семейства Windows: Microsoft Windows 8.1 и выше Серверные ОС семейства Windows: Microsoft Windows Server 2012 R2 и выше Astra Linux Common Edition: версия 2.12.40 и выше Astra Linux Special Edition: версия 1.6 и выше Ubuntu: версия 18.04 и выше Debian: версия 10 и выше
Поддерживаемые СУБД	Microsoft SQL Server: Microsoft SQL Server 2012 Service Pack 3 и выше, Microsoft SQL Server 2014 Service Pack 2 и выше, Microsoft SQL Server 2016 Service Pack 1 и выше, Microsoft SQL Server 2017 и выше PostgreSQL: версия 9.6 и выше Postgres Pro Certified: версия 11.11.1 и выше
CPU	Архитектура x86-64, процессор уровня производительности не менее Intel Core i5 6-го поколения 1,2 ГГц
RAM	Не менее 12 Гбайт
HDD	Не менее 1 Тбайт свободного пространства
NIC	Проводное или оптическое подключение 100 Мбит/с и выше

Для работы с веб-сайтом управления системой на компьютере пользователя должен быть установлен веб-браузер. В браузере должно быть включено выполнение сценариев JavaScript. Поддерживаются следующие версии веб-браузеров для настольных компьютеров:

1. Microsoft Internet Explorer версии 10.0 и выше.
2. Microsoft Edge.
3. Google Chrome версии 50 и выше.
4. Mozilla Firefox версии 45 и выше
5. Яндекс.Браузер версии 17.1 и выше.
6. Safari версии 9 и выше.

Программно-аппаратные требования для установки и корректной работы приложения StarForce Document Protector приведены в таблице.

Требования	Допустимые значения
Поддерживаемые ОС	Клиентские ОС семейства Windows: Microsoft Windows 8.1 и выше Серверные ОС семейства Windows: Microsoft Windows Server 2012 R2 и выше Astra Linux Common Edition: версия 2.12.40 и выше Astra Linux Special Edition: версия 1.6 и выше

	Ubuntu: версия 18.04 и выше Debian: версия 10 и выше
CPU	Не менее 1 ГГц, архитектура x86-64
RAM	Не менее 4 Гбайт
HDD	Не менее 1 Гбайт свободного пространства
NIC	Сетевое подключение 100 Мбит/с и выше

Программно-аппаратные требования для установки и корректной работы приложения StarForce Leak Investigator приведены в таблице.

Требования	Допустимые значения
Поддерживаемые ОС	Клиентские ОС семейства Windows: Microsoft Windows 7 и выше Серверные ОС семейства Windows: Microsoft Windows Server 2008 R2 и выше Astra Linux Common Edition: версия 2.12.40 и выше Astra Linux Special Edition: версия 1.6 и выше Ubuntu: версия 18.04 и выше Debian: версия 10 и выше
CPU	Не менее 1 ГГц, архитектура x86-64
RAM	Не менее 4 Гбайт
HDD	Не менее 1 Гбайт свободного пространства

Программно-аппаратные требования для установки и корректной работы приложения StarForce Reader приведены в таблице.

Требования	Допустимые значения
Все варианты исполнения	
HDD/ энергонезависимая память	Не менее 1 Гбайт свободного пространства
RAM	На 1 Гбайт выше минимальных требований для данной ОС
NIC	Требуется наличие сети на время активации документов
Вариант исполнения StarForce Reader Windows	
Поддерживаемые ОС	Клиентские ОС семейства Windows: Microsoft Windows 7 и выше Серверные ОС семейства Windows: Microsoft Windows Server 2008 R2 и выше

	Поддерживаются ОС для процессоров с архитектурами x86-32 и x86-64
Вариант исполнения StarForce Reader macOS	
Поддерживаемые ОС	macOS: версия 10.11 и выше Поддерживаются ОС для процессоров с архитектурой x86-64
Вариант исполнения StarForce Reader Linux	
Поддерживаемые ОС	Astra Linux Common Edition: версия 2.12.40 и выше Astra Linux Special Edition: версия 1.6 и выше Ubuntu: версия 18.04 и выше Debian: версия 10 и выше Поддерживаются ОС для процессоров с архитектурой x86-64
Вариант исполнения StarForce Reader Android	
Поддерживаемые ОС	Android: версия 5.0 и выше Поддерживаются ОС для процессоров с архитектурами ARM 32 и 64
Вариант исполнения StarForce Reader iOS	
Поддерживаемые ОС	iOS: версия 10 и выше Поддерживаются ОС для процессоров с архитектурой ARM 64

7 Роли и пользователи

Решение StarForce Content Enterprise поддерживает управление доступом на основе ролей. Система поддерживает следующие роли:

1. Оператор системы. Имеет логин и пароль для входа на сайт управления системой. Может управлять группами документов и серийными номерами для них, а также смотреть отчеты, связанные с активациями. Имеет доступ только к тем группам документов, на которые его назначил администратор системы.
2. Администратор системы. Имеет логин и пароль для входа на сайт управления системой. Может выполнять те действия, которые доступны оператору системы, без ограничений, а также управлять пользователями системы и просматривать общие отчеты.
3. Специалист, занимающийся расследованием утечек. Использует специальный серийный номер, с помощью которого он активирует документ с возможностью извлечения данных для расследования.
4. Читатель документов. Имеет права только на те группы документов, для которых у него есть серийный номер. Для читателя не создается учетной записи на сайте управления системой.

Один и тот же пользователь может объединять несколько ролей.

Права для ролей приведены в таблице:

Действие	Оператор системы	Администратор системы	Специалист, занимающийся расследованием утечек документов	Читатель документов
Чтение документов			+	+[1]
Расследование утечек			+	
Создание защищенного документа (защита документа)	+[2]	+		
Генерация и редактирование серийных номеров	+[2]	+		
Передача серийных номеров читателям	+	+		
Управление пользователями сайта		+		

Табл. 1. Права для ролей в системе

Примечания:

[1] Только для документов тех групп, для которых у читателя имеется серийный номер.

[2] Только для тех групп документов, на которые назначен данный пользователь.