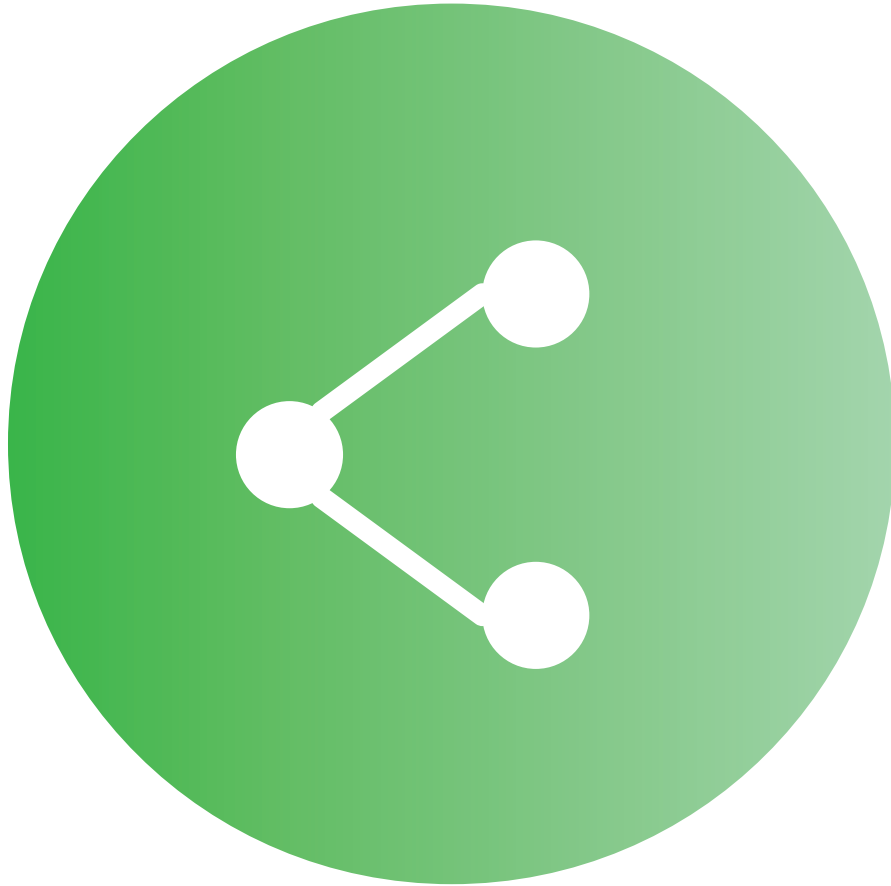




SafenSoft



## DLP Guard

Контроль и логирование действий пользователей  
на рабочих станциях в корпоративной сети

## О продукте

**SoftControl DLP Guard** осуществляет контроль и логирование действий пользователей на рабочих станциях в корпоративной сети компании, обеспечивая защиту информации от утечки путем контроля за действиями пользователей. Действия сотрудников предприятия фиксируются с возможностью получения уведомлений и создания отчетов.



## Принцип работы

SoftControl DLP Guard является программой для контроля сотрудников предприятия, обеспечивающей информационную безопасность компании путем обеспечения защиты от инсайдерских инцидентов.

Доступ сотрудника к файлам и папкам, изменение файлов, отправка документов на печать, использование USB накопителей, время работы с конкретными приложениями, ввод данных, в программах мгновенных сообщений и т.п. – все эти действия сотрудников фиксируются с возможностью создания отчетов для системного администратора, офицера службы безопасности или аналитика компании.

SoftControl DLP Guard осуществляет подробное логирование действий пользователей, позволяет настроить мониторинг файлов, папок и ключей реестра в соответствии с политиками безопасности компании для защиты информации от утечки. При попытке несанкционированного доступа к информации, сообщение об этом поступает в консоль администрирования для оперативной реакции на инцидент администратора или представителя службы безопасности.

В случае подозрения на инсайдерский инцидент или утечку информации, служба безопасности компании будет располагать информацией о полном спектре действий, осуществляемых персоналом, с возможностью удаленного просмотра и видеозаписи экрана сотрудников, попадающих под подозрение. Пробные отчеты о работе сотрудника с файловой системой, реестром, периферийными устройствами, эффективны для ретроспективного анализа и расследования, а также предупреждения инсайдерских инцидентов.

На основании отчетов о времени работы сотрудников – общем и с каждым приложением в отдельности, данных вводимых в тех или иных приложениях, может осуществляться точный контроль действий персонала компании: контроль над использованием трудовых ресурсов и стимулирование трудовой дисциплины сотрудников.

Использование политик доступа к конфиденциальной информации и информирование персонала о том, что все действия на компьютере логируются, вплоть до видеозаписи экрана, является наиболее эффективным средством защиты информации от утечки и предотвращения инсайдерских инцидентов.

## Ключевые функции

<b>Мониторинг использования файловых ресурсов компании</b>	Позволяет своевременно получать уведомления о несанкционированном доступе к конфиденциальной информации (операции чтения, создания, удаления, переименования, изменения файлов), осуществлять аналитику действий сотрудников.
<b>Мониторинг использования внешних USB-накопителей</b>	Позволяет узнать, какие файлы и когда были скопированы сотрудником на USB устройство, либо какие файлы и приложения открывались с USB накопителя (операции чтения, записи, удаления файлов).
<b>Запись экрана пользователя</b>	Программа для записи действий пользователя позволяет осуществлять записи экрана монитора, анализировать все действия пользователя в случае подозрения на инсайдерский инцидент или злонамеренные действия.
<b>Запись текста, введенного с клавиатуры для любого приложения</b>	Кей логгер – позволяет узнать, какие данные и в каком приложении сотрудник вводил с клавиатуры, пресечь утечку информации.
<b>Ведение учета отправленных сотрудником e-mail</b>	Возможно отслеживание передачи сотрудником информации во вне с помощью e-mail. Логируется название прикрепленных файлов при отправке E-mail в MS Outlook 2003.
<b>Мониторинг файлов, отправленных на принтер</b>	Позволяет отслеживать и логировать факты отправки сотрудником документов на печать.
<b>Мониторинг системного реестра</b>	Позволяет отслеживать изменения системного реестра, проводимые сотрудником или приложениями (операции чтения, создания, удаления, переименования, изменения ключей).
<b>Теневое копирование данных</b>	Возможно автоматическое сохранение оригинальных копий, изменяемых или удаляемых сотрудником файлов и ключей реестра.
<b>Система учета рабочего времени сотрудника (общего и с каждым приложением), запись действий пользователя</b>	Программа для записи действий пользователя позволяет получить необходимую информацию для отдела персонала компании, а также для руководителей. Позволяет сократить издержки, эффективно используя трудовые ресурсы компании и контролируя трудовую дисциплину сотрудников.
<b>Система учета используемых приложений</b>	Позволяет отслеживать запускаемые и используемые сотрудником приложения.
<b>Централизованное хранение данных мониторинга</b>	Вся информация о действиях сотрудников сохраняется в базе данных Service Center. На основе этой информации генерируются отчеты для ретроспективного анализа инцидентов и аналитики действий сотрудников.
<b>Получение уведомлений</b>	При доступе, изменении, удалении файлов и ключей реестра, за которыми ведется наблюдение, администратор или специалист службы безопасности получает уведомление о действиях сотрудника в консоль администрирования или на E-mail.
<b>Microsoft SQL Reporting Services</b>	Используется для генерации отчетов на основе данных мониторинга за активностью сотрудников.
<b>Сервер обновлений</b>	Позволяет использовать сервер для локального обновления клиентских компонентов программы на рабочих станциях.
<b>Удаленное управление</b>	С помощью входящей в продукт консоли администрирования осуществляется удаленная установка и деинсталляция продукта, изменение настроек.

## Целевые пользователи



### ИТ-отделы

Руководитель службы ИБ  
Офицер службы ИБ  
Руководитель ИТ-отдела  
Директор по ИТ



### Внутренние и внешние call-центры

Руководитель call-центра  
Руководитель проекта  
Супервайзер



### ТОП-менеджмент

Генеральный директор  
Руководитель отдела  
Руководитель подразделения



### Отделы кадров

Руководитель отдела кадров  
Менеджер по персоналу

## Системные требования

### Клиентские модули

**Операционные системы:** Windows 7, Windows 8, Windows 8.1, Windows 10.

**Поддерживаемые процессоры:** Intel®, AMD® (x86, x64).

**Дисковое пространство:** загрузка - 90 МБ

установка - 150 МБ

**Оперативная память:** Windows XP - 256 МБ ОЗУ

Windows 7/8/8.1/10 - 512 МБ ОЗУ

### Модули администрирования

**Операционные системы:** Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 (x86, x64).

## 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 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, промышленные предприятия, а также финансовые организации и государственные учреждения 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](http://www.safensoft.com)

Коммерческие вопросы: [sales@safensoft.com](mailto:sales@safensoft.com)

Техническая поддержка для корпоративных клиентов: [support@safensoft.com](mailto:support@safensoft.com)