Где можно использовать SecureTower®?

В локальной сети компании
В сетях со сложной архитектурой
В территориально распределённых офисах
На мобильных рабочих местах

Наши преимущества:

Система 2 в 1 (защита данных от утечек + мониторинг активности сотрудников)

В SecureTower® предусмотрена возможность разграничения прав доступа

Гибкие настройки способов перехвата (От сбора данных до сложного контроля с применением политик безопасности и блокировок)

Простая интеграция с другими системами обеспечения безопасности

Технические и системные требования*

Сервер SecureTower®
Контроль 100 рабочих станций

Процессор: 2,2+ ГГц (6 ядер и более)

Сетевые адаптеры: 1 Гбит

Оперативная память: 12 Гб и более

Жёсткий диск: раздел для операционной системы и файлов Secure Tower® — 100 ГБ;

Раздел для хранения перехваченных данных от 100 пользователей за 1 месяц — 200 ГБ.

Операционная система для серверных компонентов: Microsoft Windows Server 2008/2012/2016/2019 x64

Поддерживаемые СУБД: Microsoft SQL Server, Oracle, PostgreSQL, SQLite и MySQL

Агент
Клиентская часть на ПК контролируемых сотрудников

Конфигурация оборудования должна соответствовать рекомендациям Microsft для установленной версии операционной системы.

Операционная система для агента:

Microsoft Windows XP/Vista/7/8/10/ Server 2003/Server 2008/Server 2012/ Server 2016/ Server 2019

*Приведены усредненные расчетные данные. Системные требования зависят от заданных настроек контроля рабочих станций и срока хранения перехваченной информации.

О компании

Уже 14 лет мы занимаемся информационной безопасностью. Наша DLP-система помогает компаниям защититься от утечек конфиденциальной информации, а также контролировать работу сотрудников.

2007
Работаем с 2007 года

1000
Более 1000 клиентов по всему миру

30
Офисы и партнёры в более чем в 30 странах

1000000
Около 1 000 000 контролируемых компьютеров

Попробуйте бесплатный 30-дневный тест системы SecureTower®

ООО «Фалконгейз»
www.falcongaze.ru
sales@falcongaze.ru
Москва: +7 (499) 116-30-00
Санкт-Петербург: +7 (812) 240-17-05
Екатеринбург: +7 (343) 339-41-42
Краснодар: +7 (861) 205-51-00
Минск: +375 (17) 385-24-50

Falcongaze®

DLP система

SecureTower®

Защита бизнеса от внутренних угроз

Контроль эффективности и лояльности персонала
Контроль действий на компьютерах сотрудников
Защита данных от утечек

Возможности SecureTower®

Защита бизнеса от хищения ценной информации

Раскрытие схем мошенничества внутри компании

Контроль удалённых сотрудников

Контроль сотрудников в офисе

Выявление потенциально опасных сотрудников (анализ рисков)

Блокировка злонамеренных действий сотрудников

Защита от потери информации

Контроль эффективности и лояльности персонала

SecureTower® контролирует и записывает все действия сотрудника на компьютере: Запуск программ и приложений, посещённые сайты, подключение USB-устройств и носителей, отправляемые на печать файлы, информацию с веб-камер и микрофонов.

Полный контроль всех каналов передачи данных:

Посещённые сайты в любых браузерах
Электронная почта
Социальные сети
Мессенджеры
Облачные хранилища
Сетевые хранилища
IP телефония
Сетевые и локальные принтеры
USB-устройства
Буфер обмена

Как работает наша система?

- **Контроль каналов передачи данных**
- **Анализ всей перехваченной информации по заданным правилам безопасности**
- **Оценка лояльности персонала**
- **Информирование о нарушении правил безопасности**
- **Создание отчётов об инцидентах**
- **Приоритезация и расследование инцидентов**

Аналитические возможности SecureTower®

Контентный анализ (анализ файлов, документов по содержимому):

- Анализ текстовых файлов и отправляемого текста
- Анализ изображений (распознавание текста на изображениях, печатей, штампов)
- Анализ голосовых сообщений и звонков, распознавание речи
- Анализ по добавленным шаблонам/регулярным выражениям (распознавание пересылаемых банковских карт, фото паспорта, внутренних документов)

Анализ буфера обмена (контроль размещаемого содержимого, блокировка буфера по контенту)

Статистический анализ (учет пересылаемой информации и действий)

Анализ общих связей между сотрудниками (выявление путей распространения информации)

Анализ по цифровым отпечаткам

Распознавание замаскированных файлов

Поиск по хэш-функциям

Анализ CAD-файлов

Анализ рисков

Система анализирует деятельность сотрудников по различным параметрам и формирует список работников, представляющих повышенный риск. SecureTower® автоматически уведомляет о повышении уровня риска сотрудника, что позволяет оперативно принять меры.

Наглядные отчёты

Активность пользователя

Показывает, как сотрудник проводит рабочий день: сколько времени он активен, сколько бездействует, какие ресурсы чаще посещает, с каким типом приложений чаще взаимодействует.

Топ-отчет по пользователям

Выводит сравнительную статистику по всем сотрудникам компании исходя из выбранного критерия и временного интервала. Например, кто из сотрудников позже начинает свой рабочий день.

Сводный отчет по пользователям

Позволяет вывести сводную статистику по активности пользователей. Удобен для общей оценки активности сотрудников на рабочих местах.

Граф-анализатор взаимосвязей персонала

Отслеживает связи сотрудников внутри организации и со сторонними контактами. Данный отчёт позволяет выявить мошеннические схемы внутри организации и найти потенциальных инсайдеров.

Отчет по центру безопасности

Отражает статистику срабатывания правил безопасности с возможностью перехода к просмотру инцидентов.

Картина рабочего дня, видео- и аудиозапись

SecureTower® делает скриншоты рабочего стола в течение рабочего дня сотрудника. Кроме того, можно настроить запись с веб-камеры или микрофона сотрудника.

Все отчёты интерактивны и позволяют перейти к просмотру события для получения детальной информации.

Для всех отчетов можно создавать списки и расписания рассылок.

Расследование инцидентов

При расследовании инцидентов в SecureTower® формируются дела, в которых можно фиксировать ход расследований, определять фигурантов дела, а после завершения расследования — сделать отчёт для руководителей. Собранные данные могут быть использованы в суде в качестве доказательной базы.