

Предотвращает утечку
конфиденциальных
и персональных данных

Выявляет мошенников,
злоумышленников
и неloyальных сотрудников

Фиксирует нецелевое
использование рабочего
времени и оборудования
компании

Анализирует
бизнес-процессы
и работу персонала

SecureTower

Эффективная защита от внутренних угроз



Защитите свой бизнес от внутренних угроз с помощью
SecureTower — комплексной системы для предотвращения
утечек информации и контроля активности сотрудников

Контроль всех каналов коммуникации

Для обеспечения максимальной защиты конфиденциальной информации **SecureTower** контролирует практически все каналы коммуникации и передачи данных:

электронные письма в почтовых программах (Microsoft Outlook, Thunderbird, The Bat! и др.) на веб-ресурсах (gmail.com, mail.ru, yandex.ru и др). SecureTower контролирует передачу писем по всем стандартным протоколам, в том числе и защищенным

текстовое и голосовое общение в мессенджерах Skype, Viber, MS Lync, ICQ, Mail.ru Агент, Google Talk, Telegram, WhatsApp, Google Hangouts

веб-трафик: сообщения в социальных сетях, блогах, онлайн-чатах и на форумах; посещенные сайты и запросы по протоколам HTTP/HTTPS; файлы, передаваемые по протоколам FTP/FTPS

файлы в облачных хранилищах Dropbox, Google Drive, iCloud, OneDrive, Яндекс.Диск и Облако Mail.ru

файлы в сетевых хранилищах: на корпоративных файл-серверах, сетевых дисках и в папках

данные, передаваемые на USB-устройства различных типов

печать на локальных и сетевых принтерах

голосовое общение при использовании IP-телефонии

файлы на рабочих станциях

информацию в буфере обмена



Аналитические возможности

Учет морфологических особенностей языка

Лингвистический анализ текста, включающий контроль ключевых слов или целых фраз с учетом особенностей морфологии русского языка.

Транслитерация и нечеткий поиск

Анализ информации с полной или частичной транслитерацией, а также текста, содержащего грамматические ошибки.

Индексирование рабочих станций

Автоматический и ручной поиск конфиденциальных документов в локальной сети.

Цифровые отпечатки

Контроль утечки содержимого отдельных файлов и папок с конфиденциальной информацией. Контроль утечки содержимого баз данных.

Регулярные выражения

Анализ формализованных данных, описываемых шаблонами: номера кредитных карт и телефонов, паспортные данные, ИНН и пр. Возможность создавать любые шаблоны самостоятельно.

Статистический анализ

Анализ использования каналов коммуникаций (количество отправляемых сообщений в мессенджерах, писем, файлов и т.п.), веб-активности, активности за компьютером, активности приложений.

Анализ по словарям

Поиск конфиденциальной информации по тематическим словарям. Правило безопасности сработает, если в передаваемом тексте система обнаружит слова, словосочетания или группы слов, входящие в словарь.

Замаскированный формат файлов

Распознавание расширения файла по его содержимому. Систему не получится обмануть, изменив расширение.

Распознавание изображений

Распознавание текстовой информации на изображениях, передаваемых в любом графическом формате.

Распознавание печатей

Распознавание печатей в передаваемых файлах. Система обнаруживает печати в документах и сравнивает их с ранее загруженными эталонами.

Анализ CAD-файлов

Перехват и поиск конфиденциальных данных в чертежах, которые обрабатываются в САПР-программах.

Гибкий инструмент для создания политик безопасности позволяет комбинировать разные методы контроля и создавать многокомпонентные правила, что минимизирует процент ложных срабатываний и повышает эффективность работы службы безопасности.



Почему SecureTower?

Рациональное использование аппаратных ресурсов — компоненты системы нетребовательны к ресурсам компьютера и в то же время демонстрируют высокую производительность при обработке данных. Установка агентов на контролируемые ПК сохраняет обычную скорость отклика приложений (даже на терминальных серверах с десятками одновременно работающих пользователей).

Комплексность — один продукт решает целый спектр задач: предотвращение утечек информации, мониторинг работы сотрудников, ведение архива бизнес-коммуникаций.

Высококвалифицированная техподдержка — специалисты Falcongaze всегда готовы помочь клиентам в решении любых задач, относящихся к системе SecureTower (помощь и консультации осуществляются как удаленно, так и непосредственно у заказчика).

Простота внедрения — нет необходимости закупать дорогостоящее оборудование и вызывать специалиста, установка занимает совсем немного времени, настройка производится из одной консоли.

Простота использования — интуитивно понятный интерфейс. SecureTower эффективно работает в сетях любой сложности (в больших сетях используется многоуровневое масштабирование).

Сопровождение на всех этапах: поддержка, обучение, консалтинг и сертификация персонала.

SecureTower

защищает интеллектуальную собственность, коммерческую и конфиденциальную информацию организации, контролирует лояльность персонала, целевое использование рабочего времени и оборудования. Фиксирует активность сотрудников в любых сервисах, приложениях, на сайтах и формирует детальные интерактивные отчеты.

SecureTower контролирует максимально возможное количество каналов коммуникации, анализируя весь трафик на соответствие заданным правилам, блокирует передачу подозрительной информации и в автоматическом режиме уведомляет службу безопасности обо всех инцидентах. Система устанавливается в любую инфраструктуру сети, не требуя ее изменений, и функционирует незаметно для пользователя.

Технические и системные требования*

Сервер SecureTower

Тестирование триальной версии (контроль 25 рабочих станций)

Процессор: 2+ ГГц (2 ядра и более)

Сетевые адаптеры: 1 Гбит

Оперативная память: 6 ГБ и более

Жесткий диск: раздел для операционной системы и файлов SecureTower — 100 ГБ; раздел для хранения перехваченных данных от 25 пользователей за 1 месяц — 40 ГБ.

Операционная система для серверных компонентов:

Microsoft Windows Server 2008/2012/2016 x64

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

Агент

(клиентская часть на ПК контролируемых пользователей)

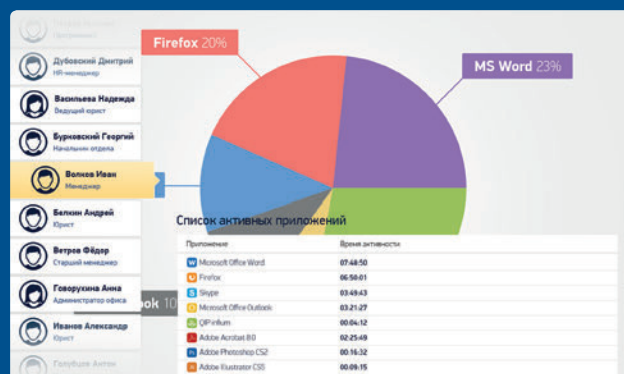
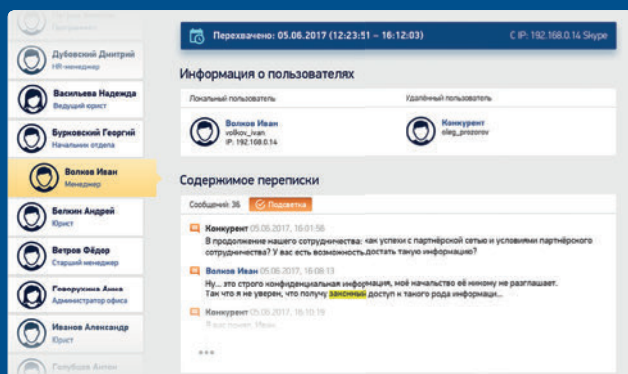
Конфигурация оборудования должна соответствовать рекомендациям Microsoft для установленной версии операционной системы.

Операционная система для агента

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

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

Контроль персонала и оптимизация бизнес-процессов

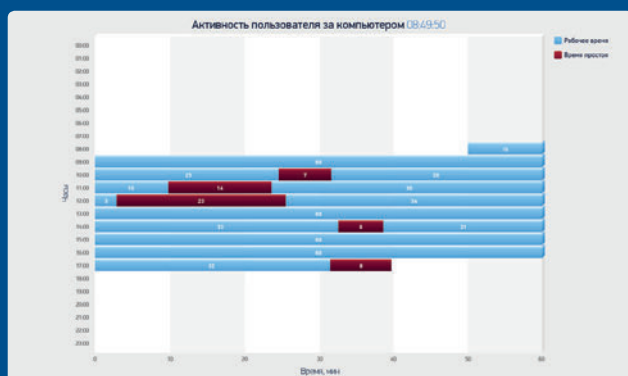


Расследование инцидентов

С помощью гибких правил система может блокировать передачу конфиденциальной информации и сообщать ответственному лицу об инциденте. SecureTower позволяет расследовать инцидент в случае утечки: выявить нарушителей, определить в их действиях умысел, предпринять меры и выработать стратегию действий. Собранные данные могут приниматься судами в качестве доказательной базы.

Выявление нелояльных сотрудников

Для выявления нелояльных сотрудников у службы безопасности есть возможность анализировать полную историю коммуникаций работников. С помощью SecureTower возможно выявить абонентов во внешней сети, ведущих нежелательную активность, например, пытающихся переманить ценные кадры или получить инсайдерскую информацию о компании.



Активность пользователя за ПК

Контроль активности пользователя за ПК мотивирует персонал к большей ответственности. Руководство получает наглядную картину того, как сотрудник проводит рабочий день: сколько времени он активен, а сколько бездействует, с какими приложениями и как активно он работает, сколько времени проводит на различных сайтах.

Гибкая система отчетности

Статистические отчеты позволяют анализировать бизнес-процессы в компании и выявлять закономерности, указывающие на нарушения принятых политик безопасности. Динамические отчеты по заданным критериям помогают оценить работу отдельных сотрудников и подразделений. Все отчеты интерактивны, что дает возможность перехода к просмотру событий и ускоряет расследование инцидентов.



Граф-анализатор взаимосвязей персонала

Граф-анализатор отслеживает контакты пользователей внутри организации и с внешними абонентами, в том числе с конкурентами. Такой инструмент позволяет выявить неформальных лидеров в коллективе, а также найти потенциальных инсайдеров в случаях, когда утечка конфиденциальной информации инициируется извне.

Фотография рабочего дня, видео- и аудиозапись

SecureTower формирует картину рабочего дня каждого сотрудника. Руководство может оценить, насколько активно сотрудник использует каналы коммуникации. Кроме того, пользователь SecureTower может удаленно подключаться к веб-камере или рабочему столу сотрудника. Для расследования инцидентов и проверки активности сотрудника предусмотрена функция видео- и аудиозаписи.

Использование SecureTower

В локальной сети предприятия

SecureTower контролирует все каналы передачи данных и предотвращает утечки конфиденциальной информации и персональных данных.

Для мобильных рабочих мест

SecureTower контролирует мобильные рабочие станции (ноутбуки и нетбуки) внутри компании и за ее пределами. Если сотрудник едет в командировку, агент **SecureTower** продолжает работать на его ноутбуке и сохраняет всю информацию, а при подключении к локальной сети передает накопленные данные на сервер.

В территориально распределенных офисах

SecureTower поддерживает работу в компаниях с территориально распределенной структурой офисов (в крупных холдингах или филиальных сетях). Внедрение, настройка **SecureTower**, а также управление системой могут осуществляться централизованно. При этом работа подразделений может быть полностью автономной, и в то же время вся перехваченная информация может передаваться в единое централизованное хранилище.

В сетях со сложной архитектурой

SecureTower надежно функционирует в компаниях со сложной архитектурой локальной сети, например в мультидоменных структурах, в сетях с кластерами терминальных серверов.

Гибкие настройки способов перехвата

Пользователь **SecureTower** может использовать несколько схем работы: перехват информации программами-агентами, установленными на компьютерах пользователей, централизованный перехват данных с использованием зеркалирования трафика или гибридный вариант, совмещающий оба способа. Возможна интеграция системы с корпоративными почтовыми серверами, а также с Proxy-серверами по протоколу ICAP.

Система разграничения прав доступа

Дает возможность гибко настроить доступ к функционалу **SecureTower** с учетом структурной и организационной иерархии компании. Позволяет обеспечить специалистов в разных областях (информационная безопасность, работа с кадрами, управленческая деятельность) подходящими инструментами для наиболее эффективного решения задач.



Возможности SecureTower

Контроль каналов передачи данных

Перехват всего входящего и исходящего трафика позволяет контролировать максимально возможное количество каналов коммуникации и минимизировать риск потенциальной утечки информации.

Анализ информации на заданные политики безопасности

Метод контентного анализа перехваченных данных позволяет в автоматическом режиме выявлять инциденты, связанные с возможной утечкой информации. Служба безопасности получает уведомление о случившемся и может незамедлительно приступить к расследованию инцидента.

Оценка лояльности и выявление мошенников

Статистический анализ позволяет оценивать сетевую активность персонала, а инструмент «Граф-анализатор взаимосвязей» — анализировать круг общения сотрудников как внутри компании, так и с внешними абонентами, выявляя и локализуя группы нелояльных работников, а также потенциальных нарушителей политики безопасности.

Обширные возможности по созданию отчетов

«Центр отчетности» дает возможность создавать разнообразные виды отчетов как по отдельным пользователям в сети, так и по всей компании в целом. Представленная в наглядном виде информация позволяет не только получить представление о положении дел в организации, но и продемонстрировать эффективность использования продукта руководству.

Контроль эффективности работы персонала

Функционал для контроля работы персонала дает возможность определить, насколько эффективно каждый сотрудник исполняет свои должностные обязанности, что, в свою очередь, позволяет оптимизировать бизнес-процессы внутри компании.

Ведение архива бизнес-коммуникаций

Позволяет создать упорядоченный архив корпоративных коммуникаций в рамках бизнес-процессов. Обратившись к архиву, можно в любой момент просмотреть историю общения всех абонентов.

Для того чтобы самостоятельно оценить богатство инструментов и эффективность системы, свяжитесь с нашими менеджерами и закажите бесплатное пилотное тестирование.



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

Минск: + 375 (17) 385 24 50

О компании

Компания «Фалконгейз» была основана в 2007 году. Является разработчиком и поставщиком высокопроизводительных решений премиум-класса в области информационной безопасности. Предлагает комплексные решения для контроля утечки и нежелательного распространения конфиденциальной корпоративной информации, адаптированные для мониторинга сетевой деятельности сотрудников.