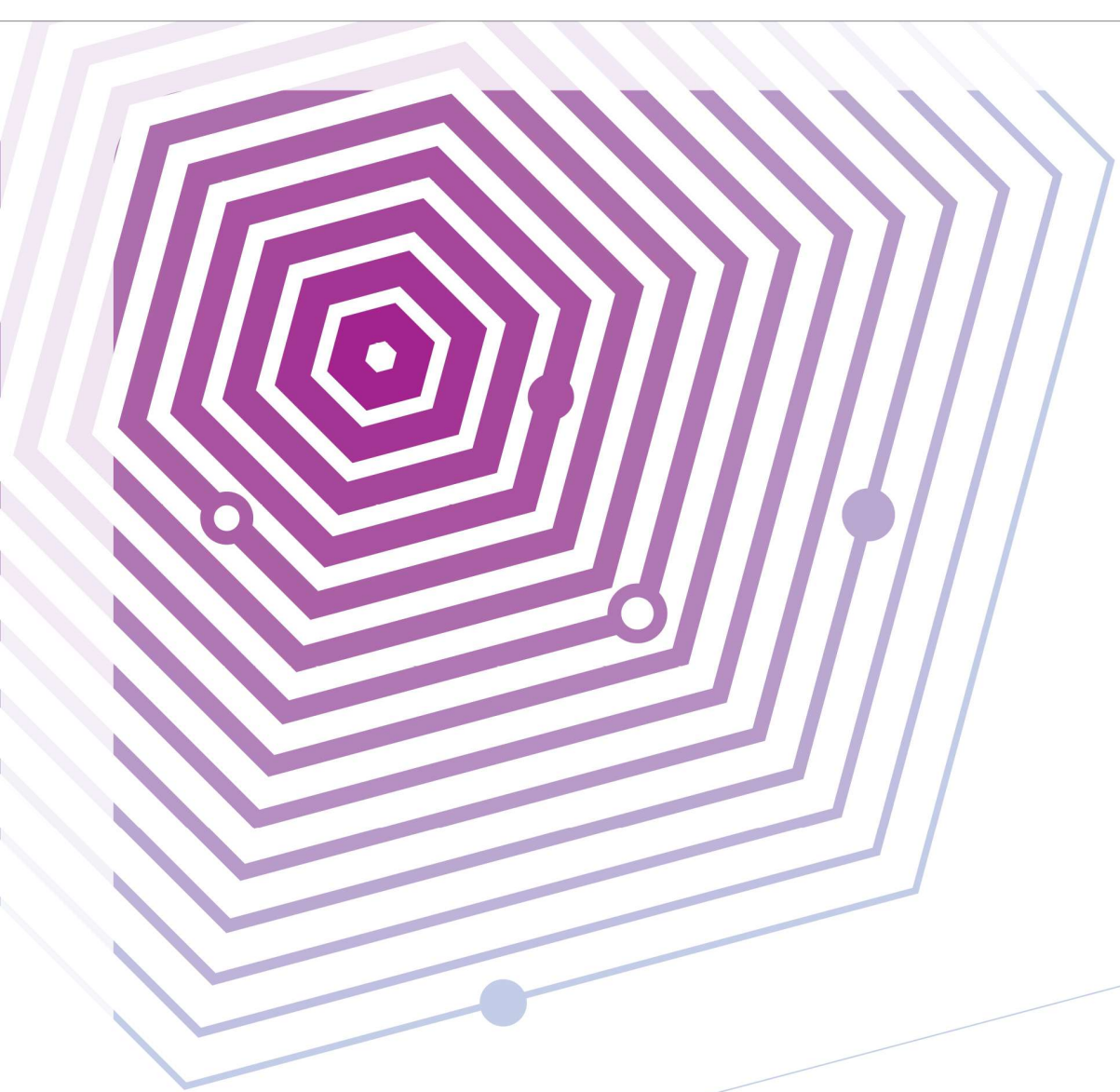

ЭФФЕКТИВНАЯ ЗАЩИТА
ОТ ВНУТРЕННИХ УГРОЗ

falcongaze

SecureTower™

Почему SecureTower?

- Защищает бизнес от хищения ценной информации
- Способствует раскрытию схем мошенничества
- Контролирует эффективность работы сотрудников
- Фиксирует подозрительную активность
- Блокирует злонамеренные действия пользователей

Возможности SecureTower

- Контроль каналов передачи данных
- Анализ информации по заданным политикам безопасности
- Оценка лояльности персонала
- Приоритизация и расследование инцидентов
- Обширные возможности по созданию отчетов

Программа позволяет комбинировать различные правила при создании политик безопасности. Это минимизирует количество ложных срабатываний и повышает эффективность работы службы безопасности

Использование SecureTower

Где?

- В локальной сети предприятия
- В сетях со сложной архитектурой
- В территориально распределенных офисах
- На мобильных рабочих местах

Преимущества

- Система разграничения прав доступа
- Минимальная нагрузка на рабочие станции
- Простая интеграция с другими системами обеспечения безопасности

Технические и системные требования*

Сервер SecureTower

Тестирование триальной версии (контроль 25 рабочих станций)
Процессор: 2,2+ ГГц (4 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 – 50 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 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/Server 2019

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

Расследование инцидентов

В SecureTower предусмотрена возможность расследовать инциденты безопасности и формировать дела, в которых можно подробно фиксировать ход расследований, выявлять фигурантов дела, а после завершения расследования – получать автоматически составленные отчеты для руководителей. Собранные данные могут использоваться в суде в качестве доказательной базы.

Анализ рисков

Модуль анализирует деятельность каждого сотрудника по заданным параметрам, автоматически генерирует отчеты для исследования тенденций поведения пользователей. Модуль позволяет специалистам отдела безопасности оценить текущие угрозы и предпринять меры для предотвращения инцидентов.

Аналитические возможности

- Транслитерация и нечеткий поиск
- Регулярные выражения
- Цифровые отпечатки
- Поиск по хеш-функциям
- Статистический анализ
- Контентный анализ
- Анализ по словарям
- Распознавание замаскированных файлов
- Распознавание голоса
- Распознавание изображений
- Распознавание печатей
- Анализ CAD-файлов

Наглядные отчеты

Активность пользователя

Контроль активности пользователя за компьютером 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.

Интерактивные отчеты

Позволяют анализировать бизнес-процессы в компании и оперативно выявлять проблемные моменты. Отчеты по заданным критериям помогают оценить работу отдельных сотрудников и подразделений. Все отчеты интерактивны и позволяют перейти к просмотру события, что ускоряет расследование инцидентов.

Граф-анализатор взаимосвязей персонала

Отслеживает контакты пользователей внутри организации и со сторонними пользователями, в том числе с конкурентами. Такой инструмент позволяет выявить неформальных лидеров в коллективе, определить круг общения, а также найти потенциальных инсайдеров в случаях, когда утечка конфиденциальной информации инициируется извне.

Картина 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 доступна также функция видео- и аудиозаписи.

Контроль всех каналов коммуникации

- Электронная почта
- Мессенджеры
- Веб-трафик
- Облачные хранилища
- Сетевые хранилища
- USB-устройства
- Сетевые и локальные принтеры
- IP-телефония
- Рабочие станции
- Буфер обмена

Более
1000
клиентов
по всему миру

Офисы
и партнеры
в более чем
30
странах

Около
1 000 000
контролируемых компьютеров

О компании

Компания «Фалконгейз» была основана в 2007 году. Мы разрабатываем и поставляем высокотехнологичный продукт в области информационной безопасности. Наше комплексное решение контролирует утечки и нежелательное распространение конфиденциальной информации, а также позволяет проводить мониторинг работы сотрудников.

Свяжитесь с нами, чтобы заказать пилотное тестирование продукта или присоединиться к нашей партнерской сети

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