falcongaze™ Системы информационной безопасности

Максимальный контроль над утечкой данных

Ваша компания активно использует в работе различные каналы передачи данных?

Ваш персонал имеет доступ к конфиденциальным документам?

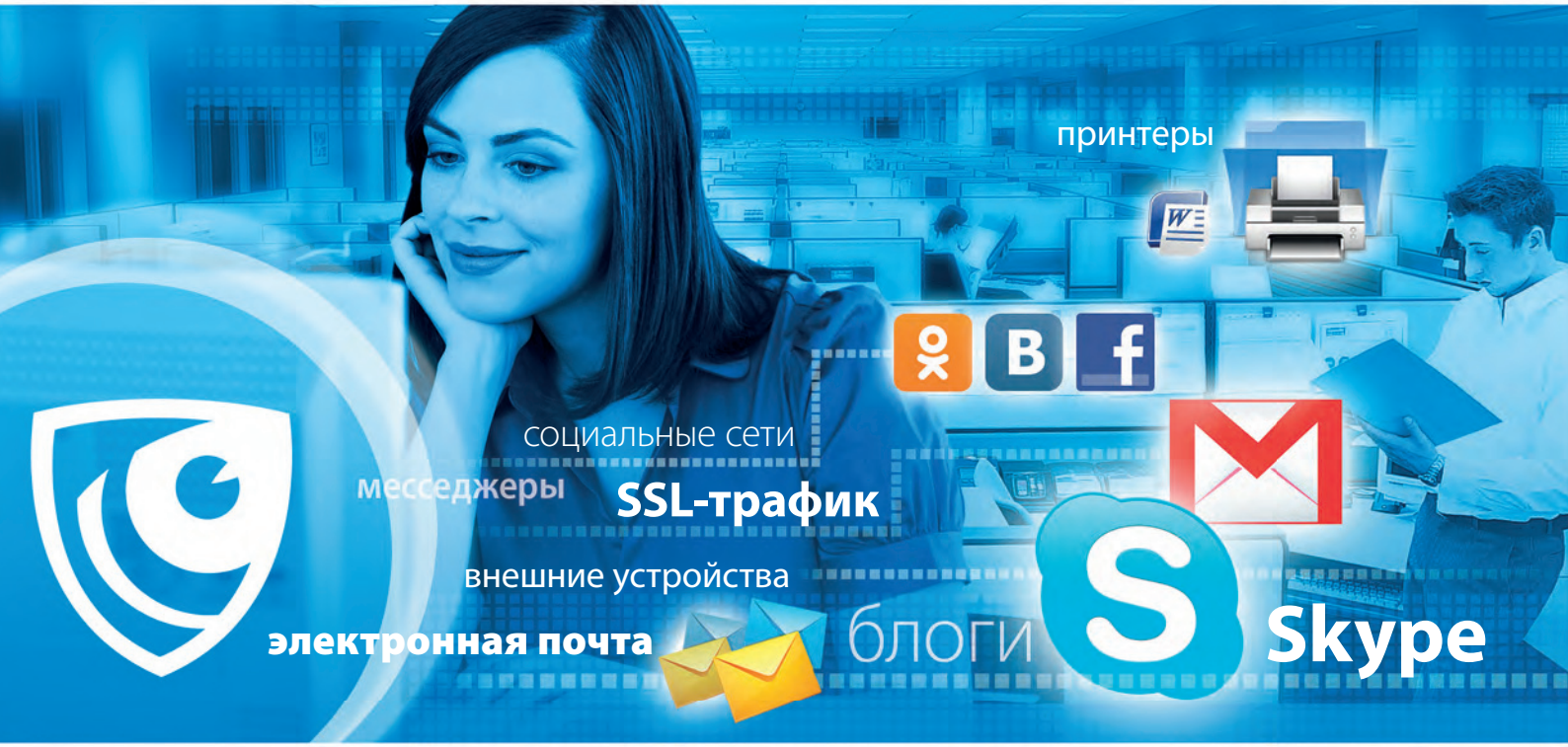
Вы не исключаете возможности, что у вас в коллективе могут быть нелояльные сотрудники?

SecureTower

Защитите свой бизнес от внутренних угроз с помощью SecureTower – комплексной системы для защиты от утечки данных и контроля активности сотрудников.

Контроль всевозможных каналов коммуникации

- **Электронные письма** почтовых клиентов, использующих протоколы POP3, SMTP, IMAP (например, MS Outlook, Thunderbird, The Bat!), электронные сообщения MS Exchange Server, IBM Lotus Notes/Domino, Kerio Connect, Sendmail, hMailServer и многих других;
- весь **веб-трафик**, включая электронные письма внешних почтовых служб (gmail.com, mail.ru, rambler.ru и т.д.), сообщения на форумах и в блогах, трафик в социальных сетях и других веб-службах;
- **сообщения мессенджеров**, использующих протоколы OSCAR (ICQ/AIM), MMP (Mail.Ru Агент), MSN (Windows Messenger), Microsoft Lync, XMPP (Jabber) (таких как Miranda, Google Talk, QIP Infium, PSI), YIM (Yahoo! Messenger), а также текстовые и голосовые сообщения в Skype;
- данные, передаваемые на **сетевые хранилища информации** (корпоративные файл-серверы, сетевые диски и папки);
- **файлы**, передаваемые по протоколам FTP, FTPS, HTTP и HTTPS, а также в программах-мессенджерах (ICQ, Windows Messenger и т.д.) или по электронной почте в качестве вложений;
- **IP-телефония** (текстовые и голосовые сообщения, передаваемые по протоколу SIP);
- **SSL-трафик**, передаваемый по шифрованным протоколам (включая HTTPS, FTPS, защищенные протоколы SSL для POP3, SMTP и мессенджеров);
- **внешние устройства** (USB-устройства, съемные жесткие диски, карты памяти и т.д.);
- печать данных на локальных и сетевых **принтерах**.



Весь трафик анализируется на соответствие заданным политикам безопасности, в случае обнаружения инцидента система автоматического оповещения **SecureTower** незамедлительно отсылает уведомления уполномоченным сотрудникам.

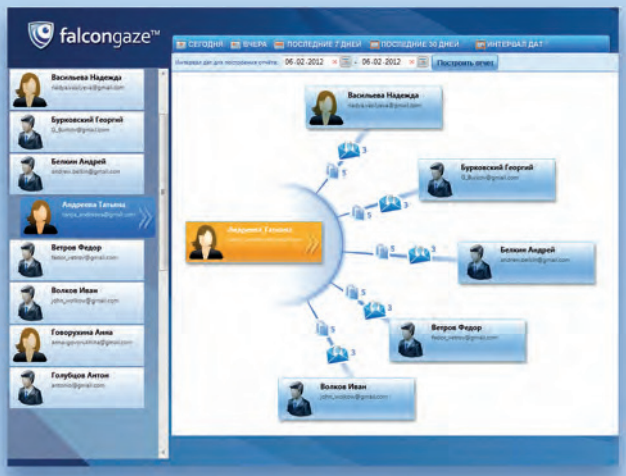
Набор предустановленных правил безопасности, включенных в комплект поставки, позволяет начать анализ данных и получать результаты сразу же после установки продукта.

Гибкий инструмент для создания новых правил дает возможность использовать разные способы контроля информации: лингвистический, статистический (в том числе и правила контроля активности процессов и приложений на компьютерах пользователей), атрибутивный, тематический контроль по словарям, цифровые отпечатки и другие. Комбинируя разные методы контроля, можно создавать многокомпонентные правила, что минимизирует процент ложных срабатываний и повышает эффективность работы службы безопасности.

Полный контроль персонала

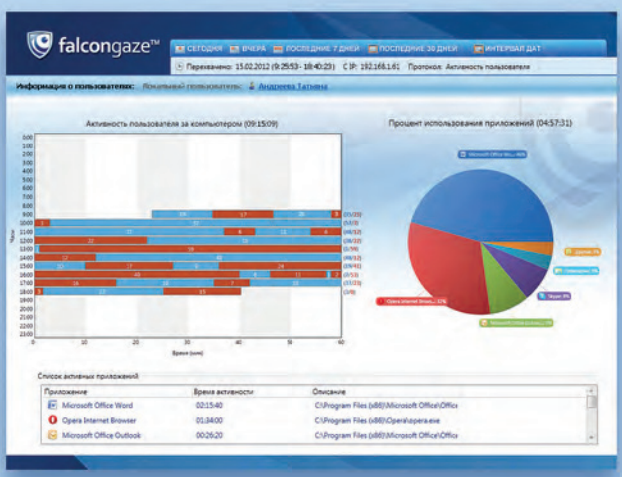
Фотография рабочего дня

SecureTower формирует фотографию рабочего дня каждого пользователя сети. Имея перед глазами такой отчет, можно оценить, насколько активно каждый из сотрудников использует те или иные каналы коммуникации. Интерактивность отчета позволяет одним кликом перейти непосредственно к прочтению отправленного или полученного письма, сообщений в мессенджере и т.д.



Граф-анализатор взаимосвязей персонала

Данный инструмент дает возможность отслеживать контакты пользователей сети между собой и внешними абонентами. Кроме того, граф-анализатор позволяет контролировать контакты с конкурентами и быстро локализовать группу потенциальных инсайдеров в тех случаях, когда утечка конфиденциальной информации инициируется извне с вовлечением в процесс нескольких сотрудников офиса.

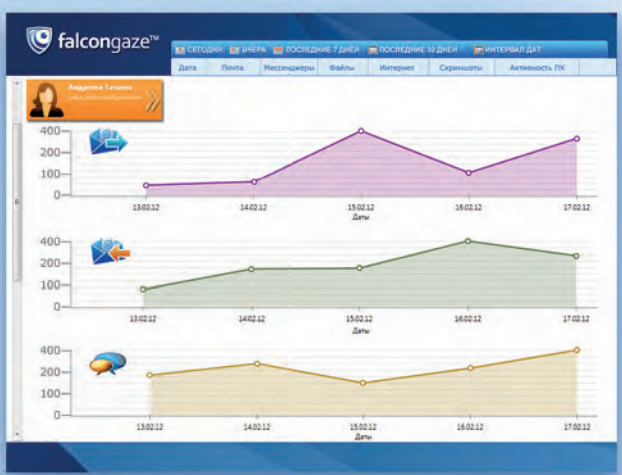


Активность пользователя за ПК

Контроль работы с приложениями и вообще всей активности пользователя за компьютером формирует наглядную картину того, как сотрудник проводит свой рабочий день. Сколько времени его компьютер активен, а сколько простаивает. С какими приложениями и как активно он работает. На выходе формируются наглядные и удобные для восприятия графические отчеты.

Снимки экранов рабочих мест

Если сотрудник работает с теми приложениями, с которыми должен работать, это вовсе не означает, что он занят своими обязанностями. Поэтому важным дополнительным функционалом, расширяющим возможности контроля персонала, является формирование снимков экранов рабочих мест с заданным временным интервалом. Просмотр галереи скриншотов позволяет оперативно оценить эффективность работы сотрудников.



Гибкая система отчетности

SecureTower формирует подробные статистические отчеты, дающие общую картину о состоянии дел в компании. Автоматически сформированные по заданным критериям отчеты можно экспортировать в распространенные форматы или сразу отправить на печать. Это позволяет не только дать оценку своей работе, но и наглядно продемонстрировать руководству эффективность и преимущества использования системы SecureTower в компании.

Преимущества внедрения SecureTower

■ **SecureTower** централизованно устанавливается и настраивается из одной консоли и не требует изменения инфраструктуры сети или покупки дорогостоящего оборудования.

■ Система **SecureTower** отличается низкими требованиями к аппаратным ресурсам компьютеров и функционирует незаметно для всех пользователей сети.

■ Установка **SecureTower** не требует вызова многочисленных технических специалистов и оплаты услуг по внедрению и консалтингу.

■ Система **SecureTower** интегрирована с Active Directory и в полной мере использует возможность установки через групповые политики домена и даже на компьютеры не находящиеся в домене. Систему отличает сверхбыстрое в сравнении с конкурентами внедрение, которое даже в крупной сети занимает всего несколько часов.

■ Совмещение в **SecureTower** различных способов анализа информации (лингвистический, статистический, атрибутивный, тематический контроль по словарям, цифровые отпечатки документов и баз данных и др.), а также возможность создания многокомпонентных правил обеспечивают контроль всего трафика на соответствие принятым в организации политиками безопасности.

■ **SecureTower** начинает полноценно функционировать сразу после установки: сбор статистики, анализ всей информации на соответствие определенным политикам безопасности, оповещение об угрозах.

■ **SecureTower** оптимизирует процесс работы с перехваченной информацией, распределяя её в сегментированные по определенным периодам хранилища. Подключение и отключение нужных баз данных и индексов производится «на лету», простой установкой маркера, и не требует перезапуска системы или каких-либо дополнительных действий.

■ Уже на стадии бесплатного тестирования наши заказчики получают возможность в сжатые сроки и при минимальных трудозатратах оценить все богатство функционала системы **SecureTower** и убедиться в ее эффективности при защите от внутренних угроз.

Технические и системные требования*:

Процессор: 2,5 ГГц и выше

Сетевой адаптер: 100 Мбит/1 Гбит

Оперативная память: не менее 4 Гб (+ 0,5 Гб на каждые 100 отслеживаемых рабочих станций)

Жесткий диск: 360 Мб свободного пространства для файлов программы и около 3–5 % от объема перехваченного трафика для файлов поисковых индексов

Microsoft .Net Framework: 4.0

Операционная система для серверных компонентов: Microsoft Windows Server 2003/ Server 2008/Server 2012 (x86 или x64)

Операционная система для компонентов клиентской части: Microsoft Windows XP/Vista/7/8/ Server 2003/Server 2008/Server 2012 (x86 или x64)

Программа поддерживает СУБД: Oracle, Microsoft SQL Server, Postgre SQL и SQLite

*Системные требования индивидуальны и зависят от характеристик сети и ее загруженности.

СЕРТИФИЦИРОВАНО ФСТЭК СЕРТИФИЦИРОВАНО


Применение SecureTower

Полный контроль сети предприятия

SecureTower контролирует утечки конфиденциальных и персональных данных, а также обеспечивает управление операционными и репутационными рисками, позволяя минимизировать возможные последствия и даже избежать их.

Контроль мобильных рабочих мест

SecureTower обеспечивает полный контроль мобильных рабочих станций и переносных компьютеров (ноутбуки, нетбуки), покидающих пределы компании. Все информационные потоки на мобильной рабочей станции будут зафиксированы и в полном объеме переданы службе безопасности при ближайшем подключении к сети организации.

Работа в территориально распределенных офисах

SecureTower поддерживает работу в компаниях с территориально распределенной структурой офисов: крупных холдингах или филиальных сетях. При этом система внедряется, настраивается и управляется централизованно. Решение позволяет контролировать утечку данных и деятельность персонала, используя удаленный доступ к нескольким ресурсам либо объединяя всю анализируемую информацию в единое централизованное хранилище.

Работа в сетях со сложной архитектурой

SecureTower надежно функционирует в компаниях со сложной архитектурой локальной сети, в мультидоменных структурах, а также в сетях с использованием терминальных серверов.

Система разграничения прав доступа

Дает возможность настроить доступ к функционалу **SecureTower** с учетом любой структурной и организационной иерархии, существующей в компании. Это позволяет обеспечивать специалистов в разных областях (информационная безопасность, работа с кадрами, управленческая деятельность) инструментом для эффективного решения задач.

Гибкие настройки способов перехвата

SecureTower предоставляет возможность использования нескольких схем работы: перехват информации с помощью программ-агентов, установленных непосредственно на компьютерах пользователей, централизованный перехват трафика с использованием зеркалирования данных и гибридный вариант, совмещающий оба этих способа.

Решаемые с помощью SecureTower задачи

Контроль каналов передачи данных

Перехват всего исходящего и входящего трафика позволяет обеспечить контроль максимально возможного количества каналов коммуникации и минимизировать риск потенциальной утечки данных.

Анализ информации на заданные политики безопасности

Инструмент для контентного анализа перехваченных данных позволяет в автоматическом режиме фиксировать инциденты, связанные с утечками конфиденциальной информации, и вовремя уведомлять службу безопасности.

Оценка лояльности сотрудников

Статистический анализ позволяет контролировать сетевую активность персонала, анализировать взаимосвязи сотрудников между собой и с внешними абонентами, выявляя и локализуя группы потенциальных инсайдеров и нелояльных сотрудников.

Контроль эффективности работы персонала

Функционал для контроля работы персонала позволяет определить, насколько эффективно каждый сотрудник исполняет свои рабочие обязанности, и предоставляет инструмент для оптимизации бизнес-процессов внутри компании.

Ведение архива бизнес-коммуникаций

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

falcongaze Системы информационной безопасности™

Россия, Москва

ООО «Фалконгейз»
Телефон: + 7 495 640 29 22
www.falcongaze.ru

Micros®

Узбекистан, Ташкент
СП *"UCD Micros"*
Телефон*: + 99871 200-34-34*
www.micros.uz

О компании

Компания **Falcongaze** была основана в 2007 году и является разработчиком и поставщиком высокопроизводительных решений премиум-класса в области информационной безопасности. Компания предлагает комплексные решения для контроля утечки и нежелательного распространения конфиденциальной корпоративной информации, адаптированные для мониторинга сетевой деятельности сотрудников.