DLP система

Falcongaze® SecureTower®

Защита информации и мониторинг активности персонала

О компании

Компания Falcongaze разрабатывает технологии и DLP-систему для защиты компаний от утечек конфиденциальной информации и обеспечения контроля эффективности и лояльности сотрудников. Главный продукт компании — DLP-система SecureTower

15

15 лет обеспечиваем информационную безопасность

1000000

около 1 000 000 компьютеров под защитой

1000

более 1000 клиентов в 20 странах

200

200 сотрудников, объединенных общей целью — сделать бизнес безопаснее

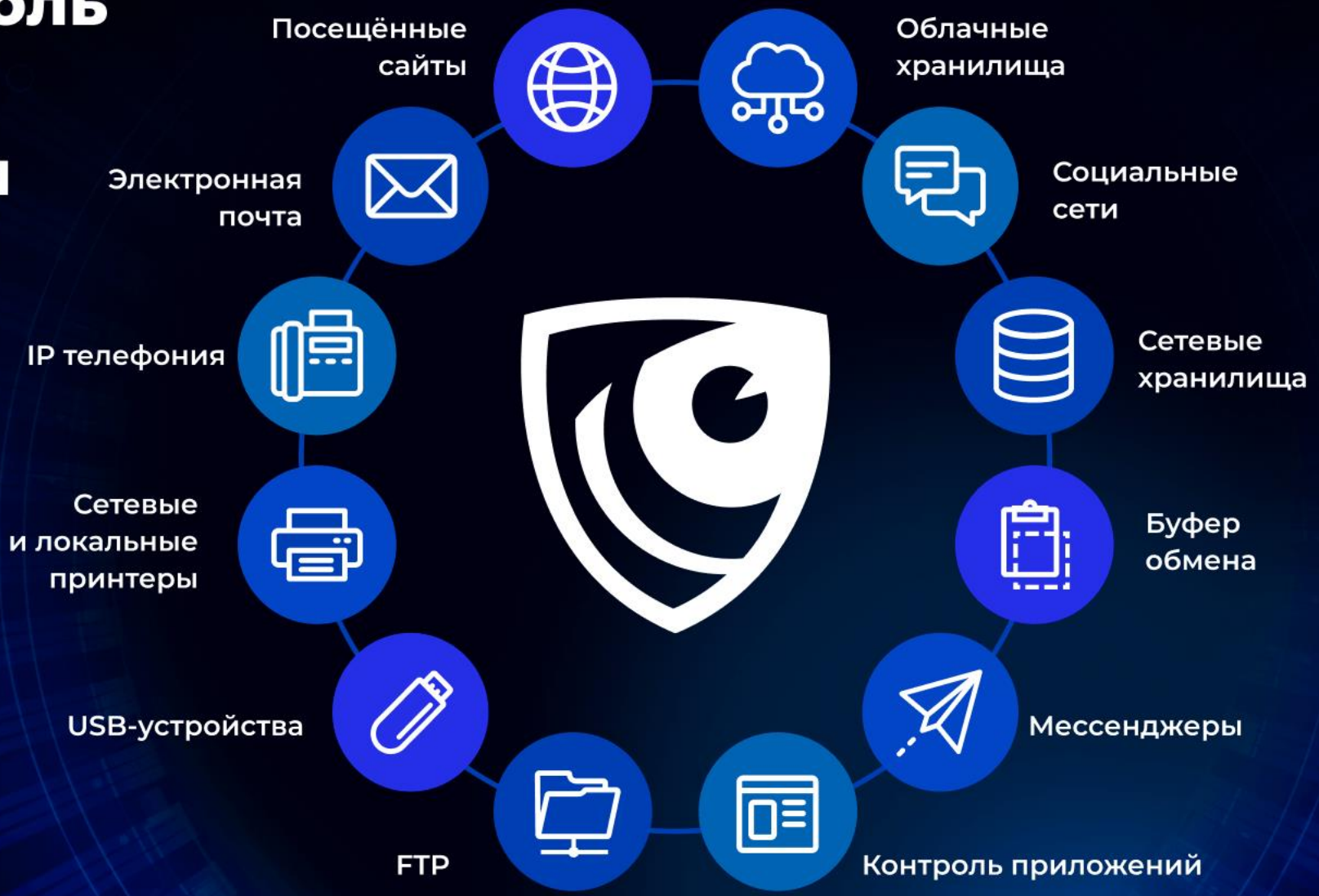
falcongaze

Что такое DLP-система SecureTower?

Система позволяет отслеживать и предотвращать обмен информацией ограниченного доступа внутри корпоративной сети, а также возможные утечки данных за её пределы

falcongaze

Полный контроль всех каналов коммуникации



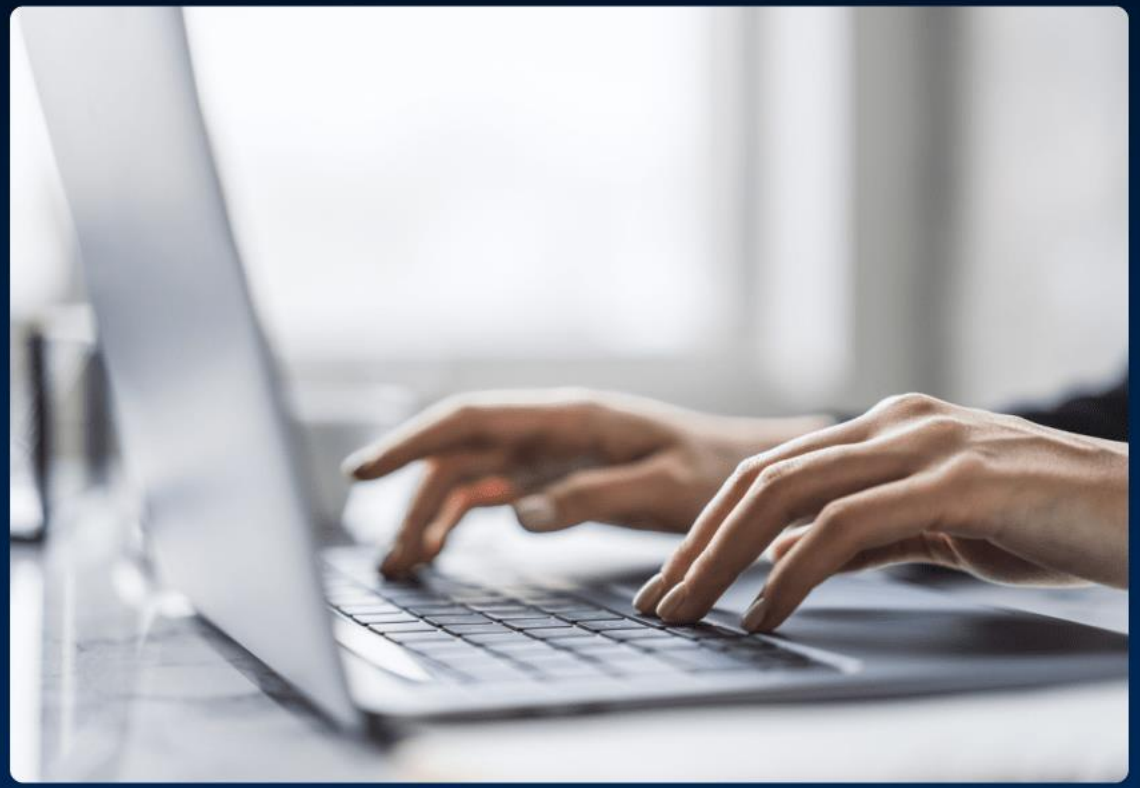
Кейс 1

falcongaze

Нелояльность сотрудников | Утечка информации

Утечка входящих лидов к конкурентам

Любая компания может столкнуться с утечкой конфиденциальной информации. В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось обнаружить передачу входящих лидов конкурентам, а также выявить виновного в утечке.



Проблема

Компания, специализирующаяся на продаже CRM-систем, обнаружила существенное снижение выручки — «горячие» клиенты один за другим перестали покупать продукт. Позже выяснилось, что они приобретали систему у конкурентов по сниженной цене. Компания начала внутреннее расследование.

Кейс 1

falcongaze

Решение

Чтобы найти причину утечки лидов, компания приобрела SecureTower. Сразу после установки система начала контролировать действия менеджеров за рабочими компьютерами, в том числе действия удаленных сотрудников. Кроме того, было создано правило безопасности, которое должно было сработать, если сотрудник отправит письмо с вложением на почтовый адрес конкурентов.

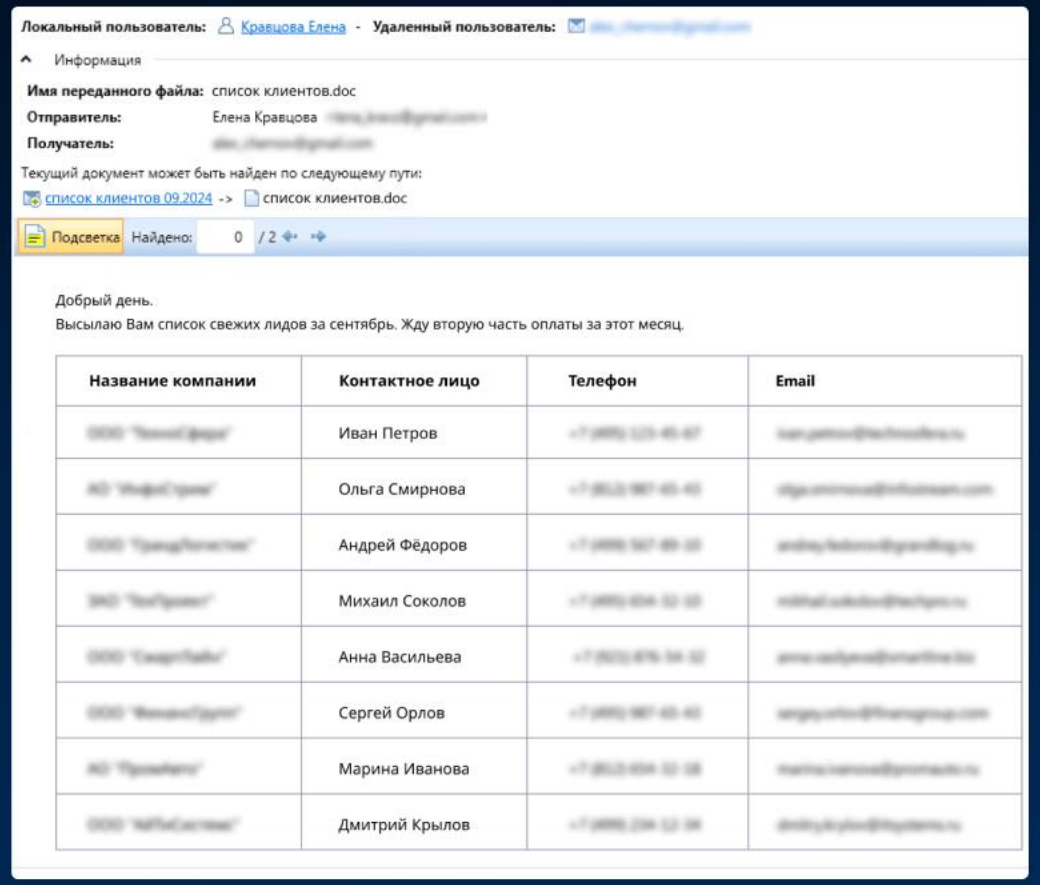
Система сообщила о нарушении спустя трое суток после установки: менеджер отдела продаж отправила письмо с вложенным документом на e-mail конкурирующей организации. Используя функционал SecureTower, офицер по безопасности проанализировал содержание письма и обнаружил, что менеджер передала списки лидов неизвестному.

Результат

- Установлен факт передачи чувствительной информации
- Выявлены нелояльные сотрудники
- Настроена блокировка передачи конфиденциальных документов
- Усилен контроль за процессом обработки лидов

Модули, которые были использованы:

- Политики безопасности
- Активность пользователей
- Комбинированный поиск
- Расследования



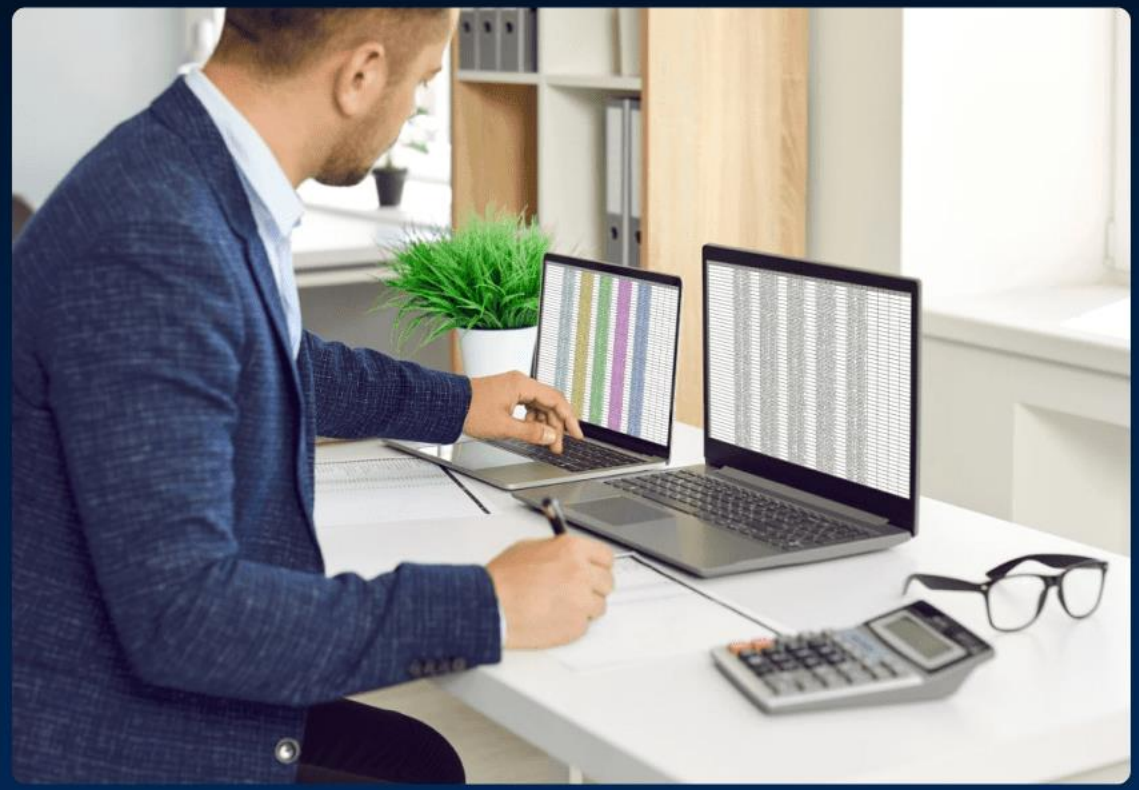
Модуль «Политики безопасности» (область поиска — почта, мессенджеры)

Кейс 2

falcongaze

Нелояльность сотрудников | Утечка информации | Высокие технологии

Предотвращение хищения данных о клиентах компании



В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось выявить факты нарушения трудового распорядка и предотвратить попытку хищения данных о клиентах компании.

Проблема

Склады и офисы компании-клиента распределены по всей России, и контролировать соблюдение трудового распорядка в подразделениях довольно проблематично. Помимо этого, за годы работы на рынке была собрана обширная горячая клиентская база, выстроены отношения с поставщиками.

Кейс 2

falcongaze

Решение

Для защиты данных от утечек и контроля за активностью персонала компания приобрела SecureTower.

Система перехватывала данные в большинстве каналов коммуникации. Помимо этого, она мониторила активность сотрудников: начало и завершение работы, контроль запускаемых приложений, время простоя компьютера и проч.

Удалось подтвердить, что несколько сотрудников нарушали трудовой распорядок: ежедневно опаздывали, уходили раньше, решали свои личные вопросы в рабочее время.

Также SecureTower зафиксировала факт копирования нескольких больших фрагментов данных о клиентах в текстовый документ облачного хранилища.
Попытка копирования была пресечена заранее настроенным правилом блокировки.

Результат

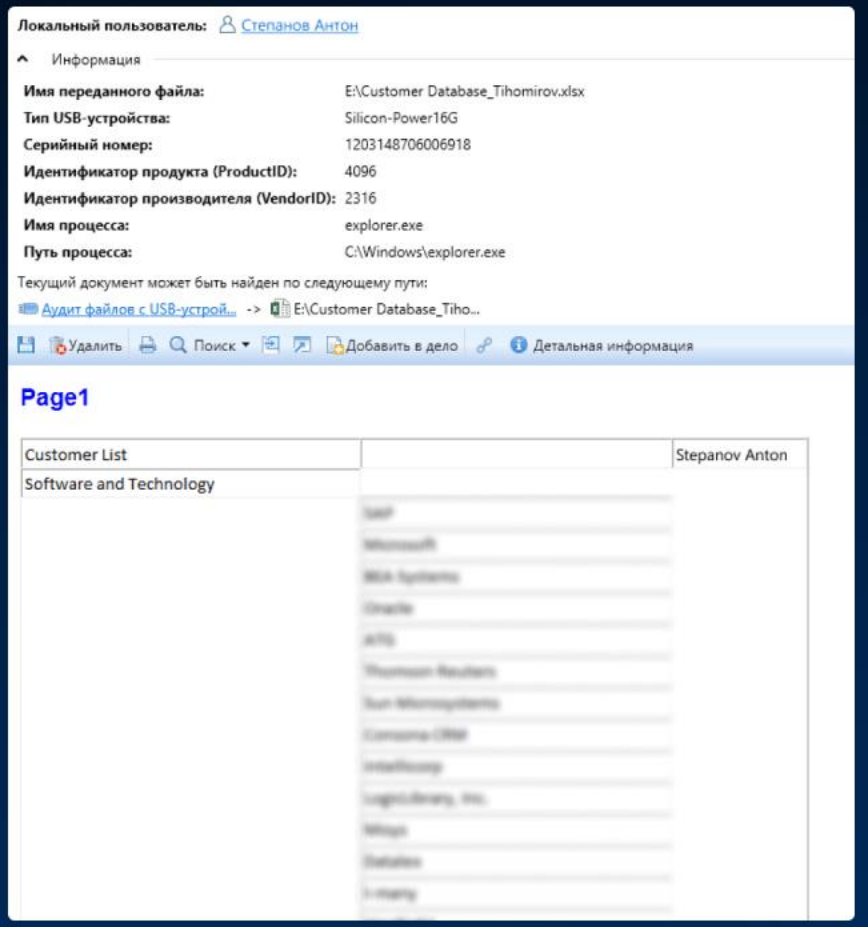
- Подтвержден факт злостного нарушения трудового распорядка
- Пресечена попытка хищения данных о клиентах компании

Модули, которые были использованы:

Комбинированный поиск

Активность пользователей

Агенты (Консоль Администратора)



Комбинированный поиск (Область поиска - почта, мессенджеры)

Кейс 3

falcongaze

Расходование ресурсов компании | Непродуктивная деятельность

Выявление сотрудников-фрилансеров

В этом кейсе мы разберем, как на этапе бесплатного тестирования DLP-системы Falcongaze SecureTower удалось установить факт нецелевого использования рабочего времени и программного обеспечения компании.

Проблема

Компания-клиент работает в проектной сфере. Одна из проблем — в конструкторском отделе постоянно срывались сроки исполнения заказов. Как итог, клиенты уходили, планы не выполнялись.

Сотрудники конструкторского отдела объясняли срывы сроков острой нехваткой времени из-за необходимости постоянно вносить правки в уже переданные на реализацию проекты.

Главный конструктор, учитывая этот факт, рассчитывал сроки выполнения проектов с большим запасом. Тем не менее, сотрудники не успевали.

Кейс 3

falcongaze

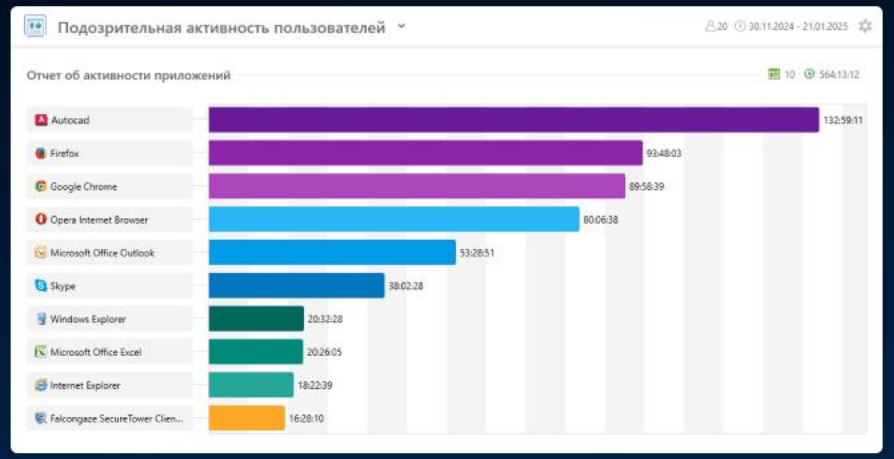
Решение

Компания установила пробную 30-дневную версию SecureTower.

Сперва был проанализирован отчет «Табель рабочего времени» — время начала и завершения работы совпадало с установленным графиком.

Затем в модуле «Отчеты» проанализировали, какие приложения запускают сотрудники. На первом месте значился процесс программы Autocad.

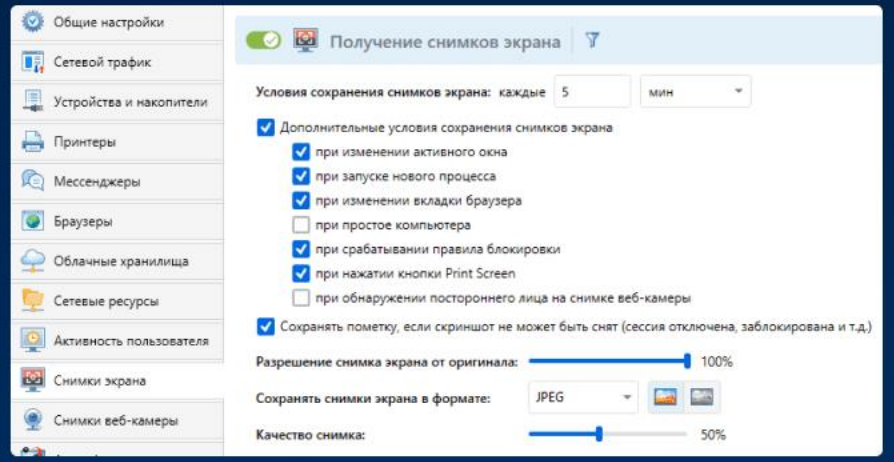
Далее с помощью снимков экрана, которые система выполняла на рабочих станциях персонала каждые 5 минут, установили, что работа ведется не над проектами компании — попавшие на снимки чертежи не имеют отношения к текущим проектам компании.



Модуль «Отчеты» (Отчет об активности пользователей)

Результат

- Выявлен факт нецелевого использования рабочего времени и программного обеспечения компании
- Сотрудников-нарушителей подвергли дисциплинарному взысканию



Консоль администратора (Настройки профиля агентов - Настройка получения снимков экрана)

Модули, которые были использованы:

Политики безопасности

Отчеты

Кейс 4

falcongaze

Нелояльность сотрудников | Утечка информации | Высокие технологии

Борьба с играми на рабочем месте

Коллектив на работу приходит вовремя, все сидят по рабочим местам, однако это не помогает — задачи решаются медленно, сроки постоянно приходится сдвигать, из-за чего компания теряет клиентов. Как руководителю быть уверенным, что сотрудник тратит свое рабочее время не напрасно?

Проблема

Проектная организация установила DLP-систему Falcongaze SecureTower и сразу настроила политики безопасности на отслеживание эффективности рабочего времени. Плюсом ST является большое разнообразие отчетов, а самым используемым стал «Сводный отчет по пользователям». Долгое время показатели отчета не привлекали внимания, однако за последние два месяца данные по трем сотрудникам ухудшились. Был зафиксирован рост нецелевой веб-активности в магазинах компьютерных игр Steam и Yandex Games.

Кейс 4

Решение

Отследить историю нарушений трудового распорядка смогли с помощью функционала «Активность пользователя». Все полученные доказательства игр на работе были зафиксированы через «Конструктор дела».

Для профилактики аналогичных инцидентов активировали предустановленные политики безопасности, фиксирующие посещение игровых ресурсов: «Посещение сайтов о видеоиграх (категории сайтов)» и «Игровые сервисы (категории приложений)». Эти действия позволили обеспечить контроль за подобной активностью для всего коллектива.

Результат

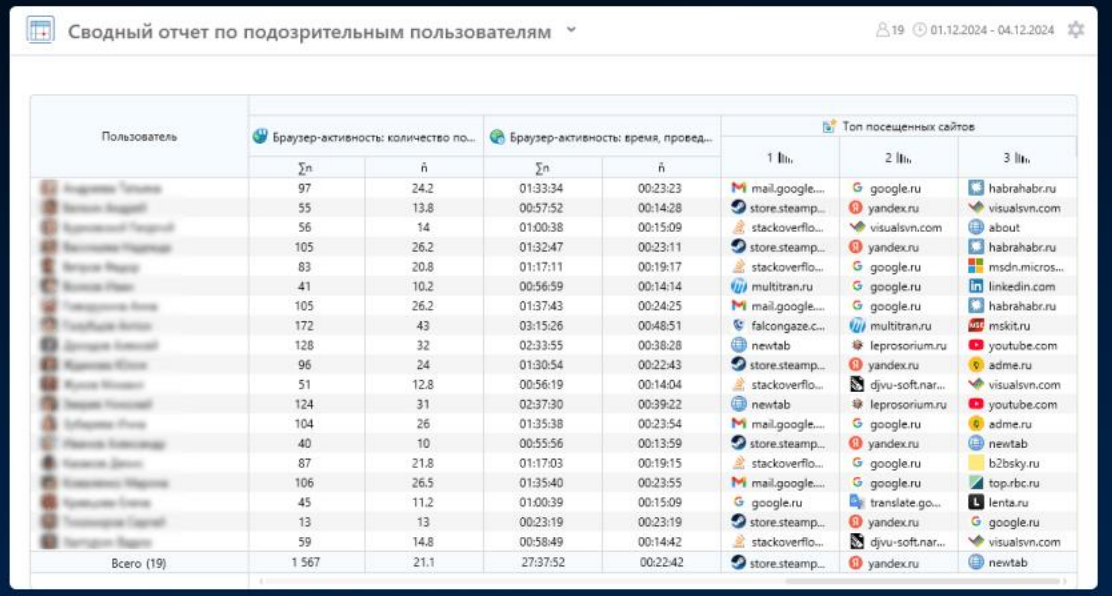
- Доказаны нецелевые траты рабочего времени
- Заведены личные дела сотрудников

Модули, которые были использованы:

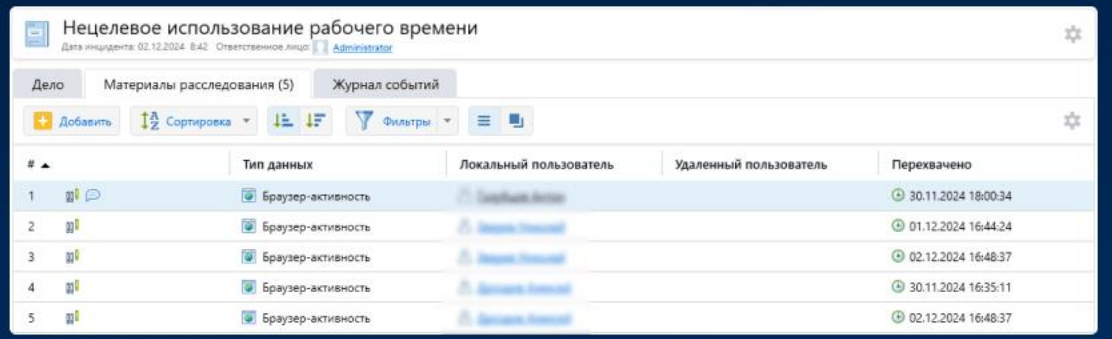
Политики безопасности

Отчеты

Расследования



Модуль «Отчеты» (Сводный отчет)



Модуль «Расследования»

Спасибо
за внимание!

Falcongaze®

www.falcongaze.com
Москва: +7 (499) 1163000
Санкт-Петербург: +7 (812) 2401705
Екатеринбург: +7 (343) 3394142
Минск: +375 (17) 3111014