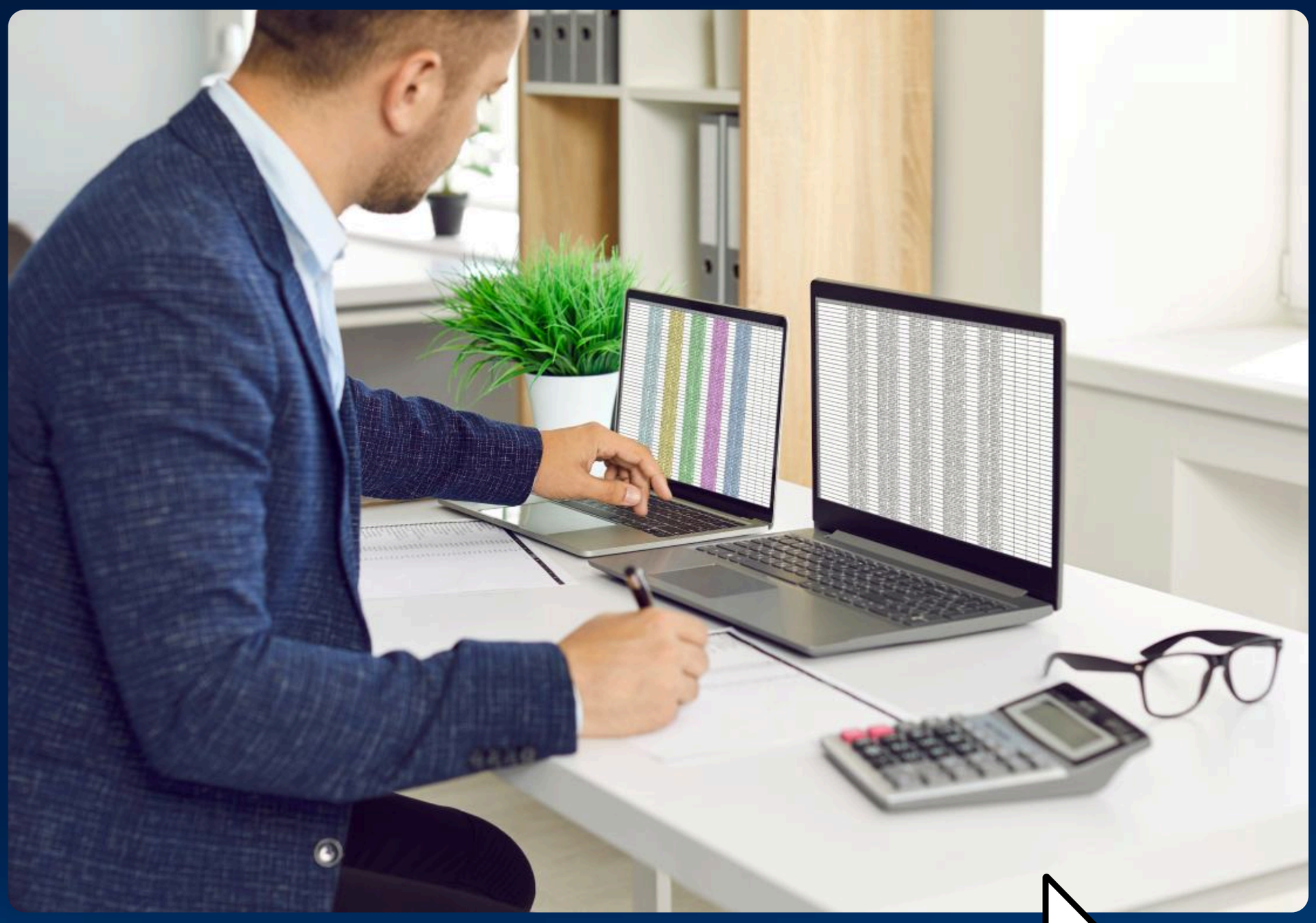
falcongaze®

Кейс клиента

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

Компания-клиент специализируется на оптовой продаже строительных материалов.

Склады и офисы компании распределены по всей России, и контролировать соблюдение трудового распорядка в подразделениях довольно проблематично. Помимо этого, за годы работы на рынке была собрана горячая клиентская база, выстроены отношения с поставщиками. Это огромный массив информации о партнерах и клиентах, их персональные и контактные данные, история сотрудничества, особенности коммуникации, цены и проч.

Было принято решение организовать защиту ценных данных от утечек и внедрить систему мониторинга активности персонала.

Решение

Для защиты этих данных от утечек, а также контроля за активностью персонала в течение рабочего дня компания приобрела SecureTower.

Система круглосуточно перехватывала и анализировала все данные в следующих каналах коммуникации:

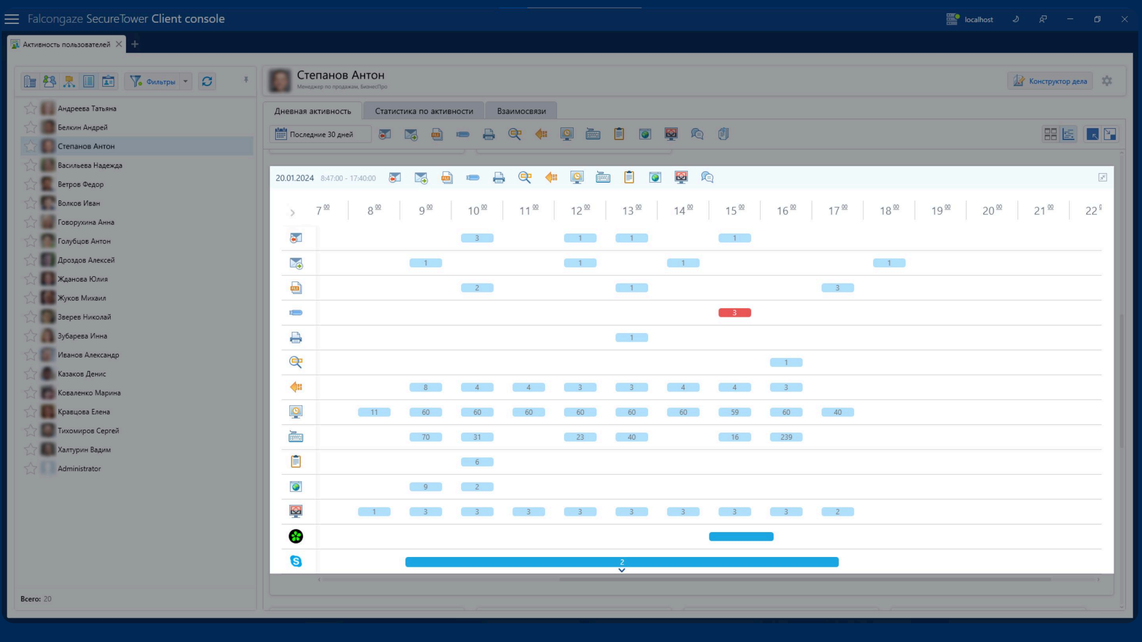
- электронная почта и ее веб-версии по всем стандартным протоколам и их зашифрованным аналогам;
- мессенджеры;
- облачные хранилища;
- подключаемые USB-устройства различных типов;
- локальные и сетевые принтеры;
- буфер обмена и проч.

Помимо этого, SecureTower мониторила активность офисных сотрудников компании в течение дня: начало и завершение работы, контроль запускаемых приложений, время простоя компьютера и проч.

На заметку! Установка агентов DLP-системы на рабочие станции может производиться удаленно, незаметно для сотрудников.

Уже в течение первой недели использования SecureTower удалось подтвердить, что несколько сотрудников регионального представительства, включая руководителя, злостно нарушали трудовой распорядок: ежедневно опаздывали, уходили значительно раньше, решали свои личные вопросы, которые занимали не один час времени. Руководителя отдела лишили премии и дали указание провести беседу с подчиненными. Вместе с этим, были настроены правила безопасности, которые помогли бы оценить эффект от проведенной беседы.

Нарушения прекратились. Тем не менее, руководитель отдела в штыки принял ситуацию. Спустя неделю DLP-система зарегистрировала несколько нарушений предустановленных правил безопасности, в том числе «Негативные настроения в коллективе».



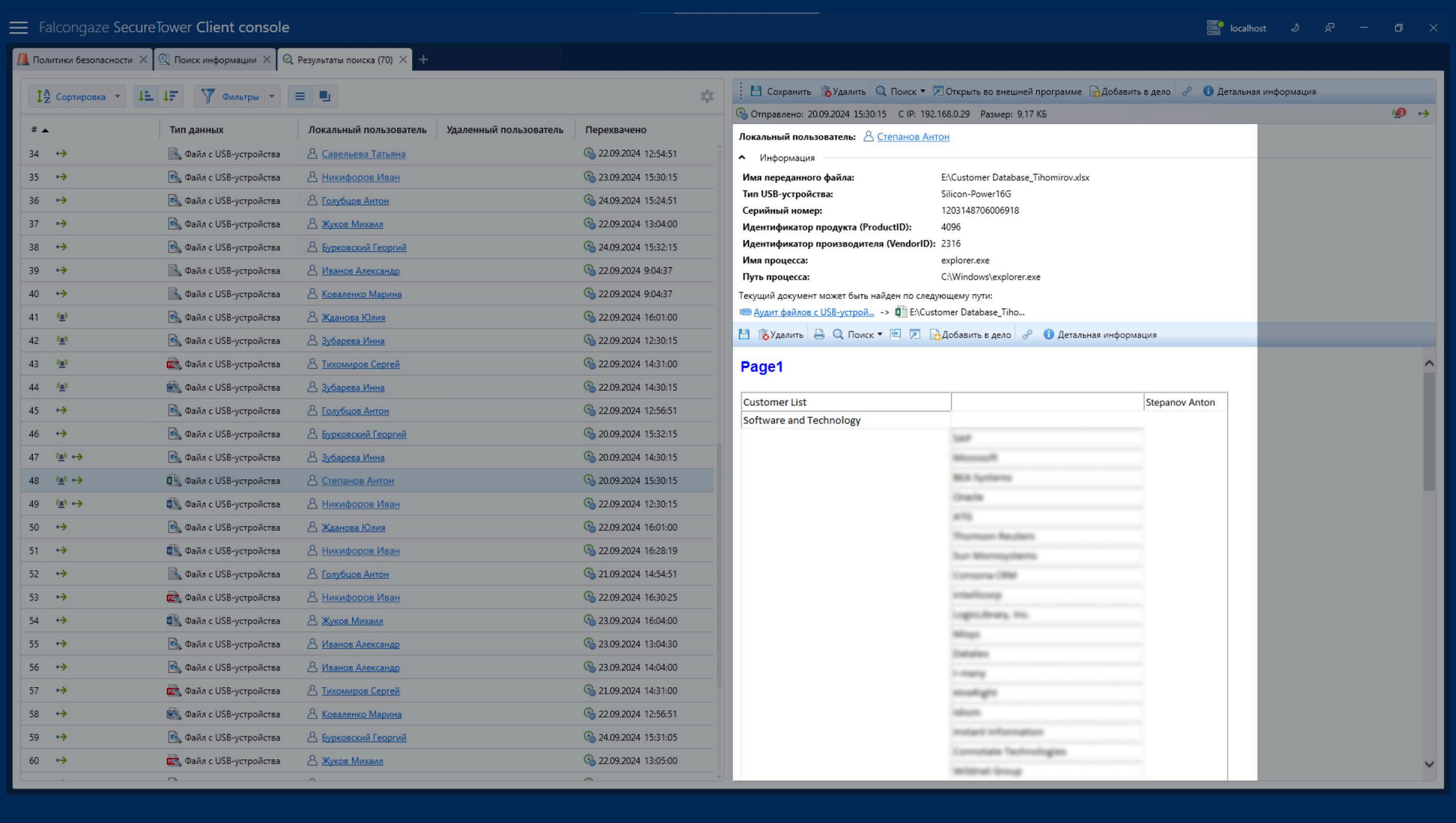
Модуль «Активность пользователей» (дневная активность)

Приняли решение проанализировать перехваченные переписки. В ходе рассмотрения инцидента стало понятно, что руководитель негативно воспринял ужесточение контроля: в переписке с одним из коллег он обсуждал сложившуюся ситуацию, грозился в ближайшее время уволиться и забрать с собой клиентов, с которыми продолжит работать уже на новом месте.

Было принято решение усилить контроль за сотрудником, учитывая возможность кражи клиентской базы и чувствительной информации. Для обеспечения безопасности данных для этого пользователя создали правило блокировки, не позволяющее копировать информацию на внешние ресурсы по всем каналам коммуникации.

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

Сотрудник попытался скопировать клиентскую базу в облачное хранилище.



Комбинированный поиск (Область поиска - почта, мессенджеры)

Спустя несколько дней SecureTower зафиксировала факт копирования в буфер обмена нескольких больших фрагментов данных о клиентах и попытки вставить их в текстовый документ облачного хранилища.

Попытка копирования была пресечена заранее настроенным правилом блокировки.

Результат

- **Подтвержден факт злостного нарушения трудового распорядка**

  Трудовая активность в течение дня взята под контроль, в том числе в региональных представительствах. Нарушителям вынесено предупреждение.

- **Пресечена попытка хищения данных о клиентах компании**

  Система заблокировала попытку копирования данных о клиентах на внешний сервис. Нелояльный сотрудник был уволен.

Модули, которые были использованы:

- Комбинированный поиск
- Активность пользователей
- Агенты (консоль Администратора)

falcongaze®