



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

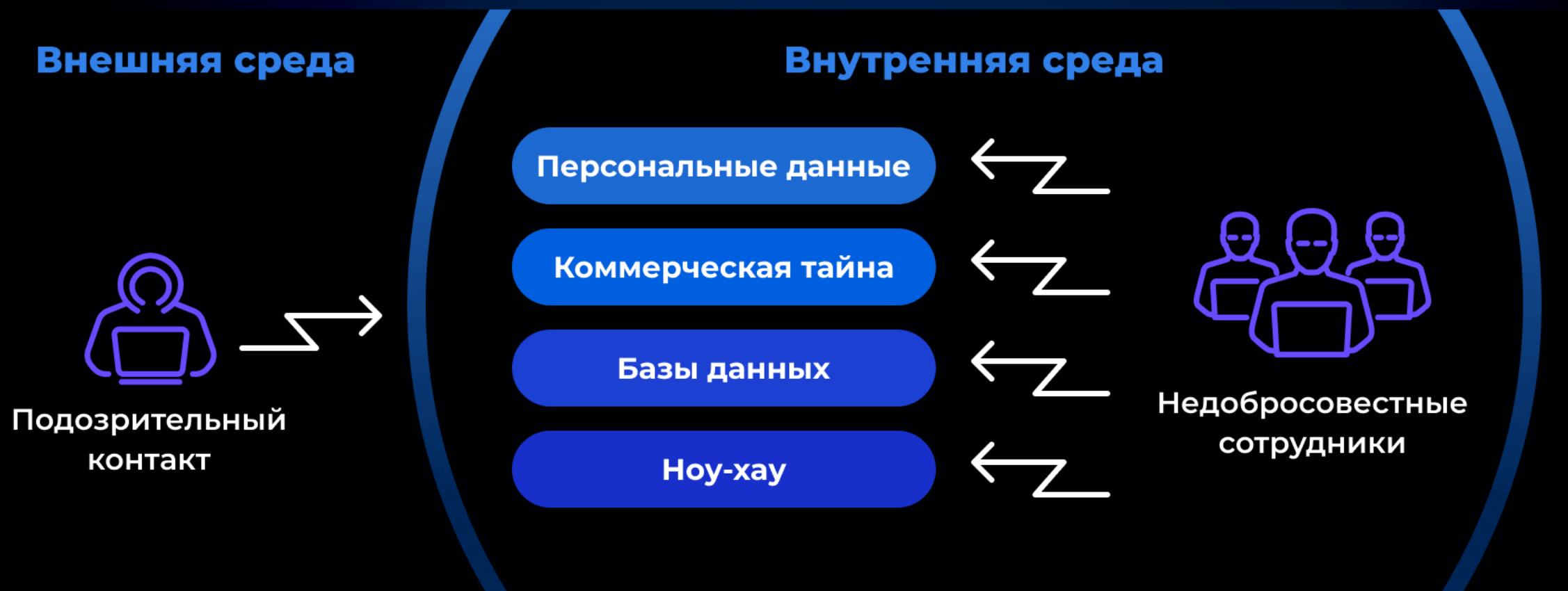


200

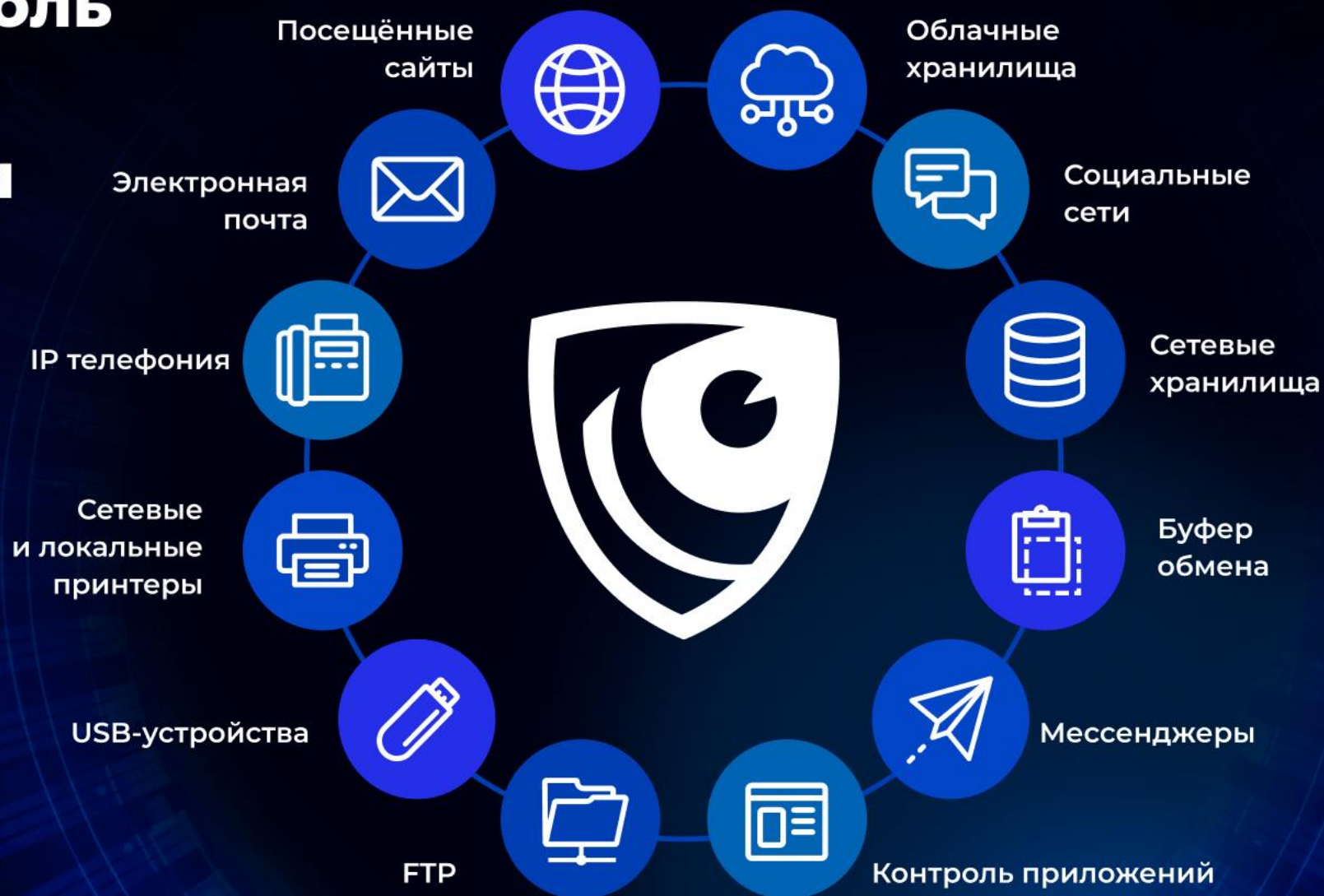
200 сотрудников, объединенных
общей целью — сделать
бизнес безопаснее

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



Полный контроль всех каналов коммуникации



Нелояльность сотрудников

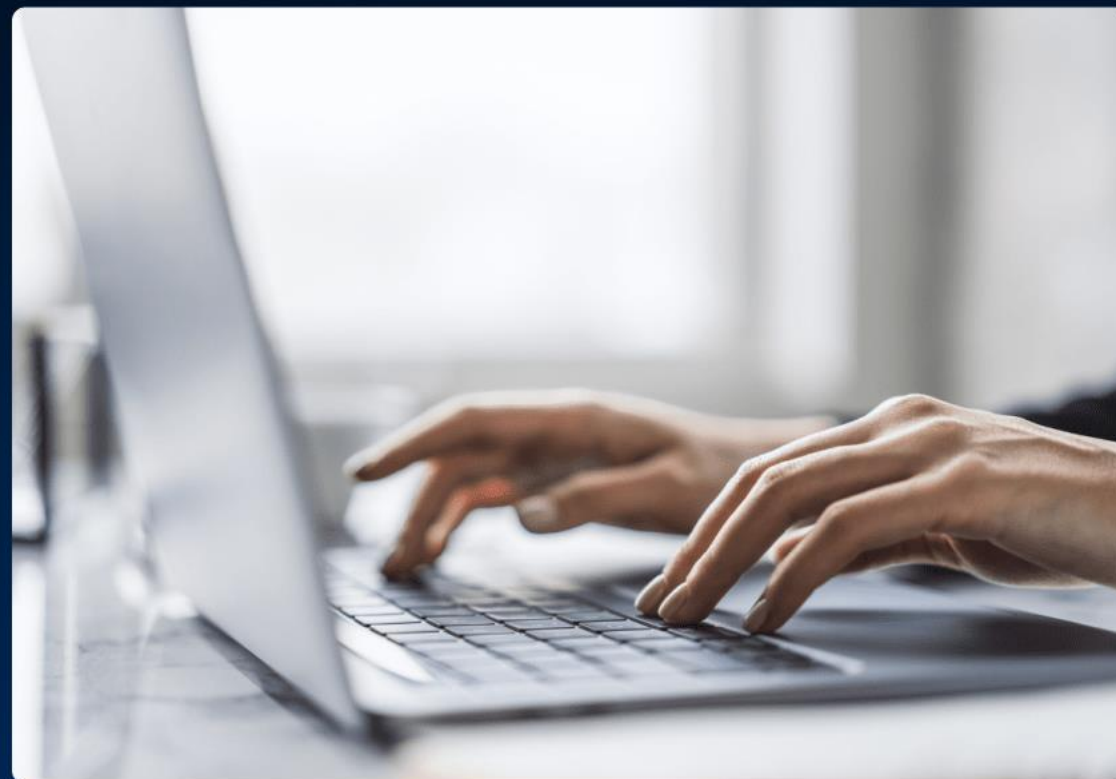
Утечка информации

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.



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 отправил 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**

Локальный пользователь:  [Кравцова Елена](#) - Удаленный пользователь:  [info@compagny.com](#)

Информация

Имя переданного файла: список клиентов.doc

Отправитель: Елена Кравцова [info@compagny.com](#)

Получатель: [info@compagny.com](#)

Текущий документ может быть найден по следующему пути:
 [список клиентов 09.2024](#) ->  [список клиентов.doc](#)

Подсветка Найдено: 0 / 2 

Добрый день.
Высылаю Вам список свежих лидов за сентябрь. Жду вторую часть оплаты за этот месяц.

Название компании	Контактное лицо	Телефон	Email
ООО "Альфа Групп"	Иван Петров	+7 (800) 123 45 67	ivan.petrov@alphagroup.ru
АО "Бета Систем"	Ольга Смирнова	+7 (812) 987 65 43	olga.smirnova@betasystems.com
ООО "Гамма Технологии"	Андрей Фёдоров	+7 (800) 567 89 10	andrey.fedorov@gammatech.ru
ЗАО "Дельта Сервис"	Михаил Соколов	+7 (800) 456 78 90	mikhail.sokolov@deltaservice.ru
ООО "Европа Трейд"	Анна Васильева	+7 (800) 345 67 89	anna.vasilyeva@eurotrade.ru
ООО "Восток Групп"	Сергей Орлов	+7 (800) 987 65 43	sergey.orlov@vostokgroup.com
АО "Глобалент"	Марина Иванова	+7 (812) 456 78 90	marina.ivanova@globalent.ru
ООО "Импульс Систем"	Дмитрий Крылов	+7 (800) 234 56 78	dmitry.kravlov@impulssystems.ru

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

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.



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:



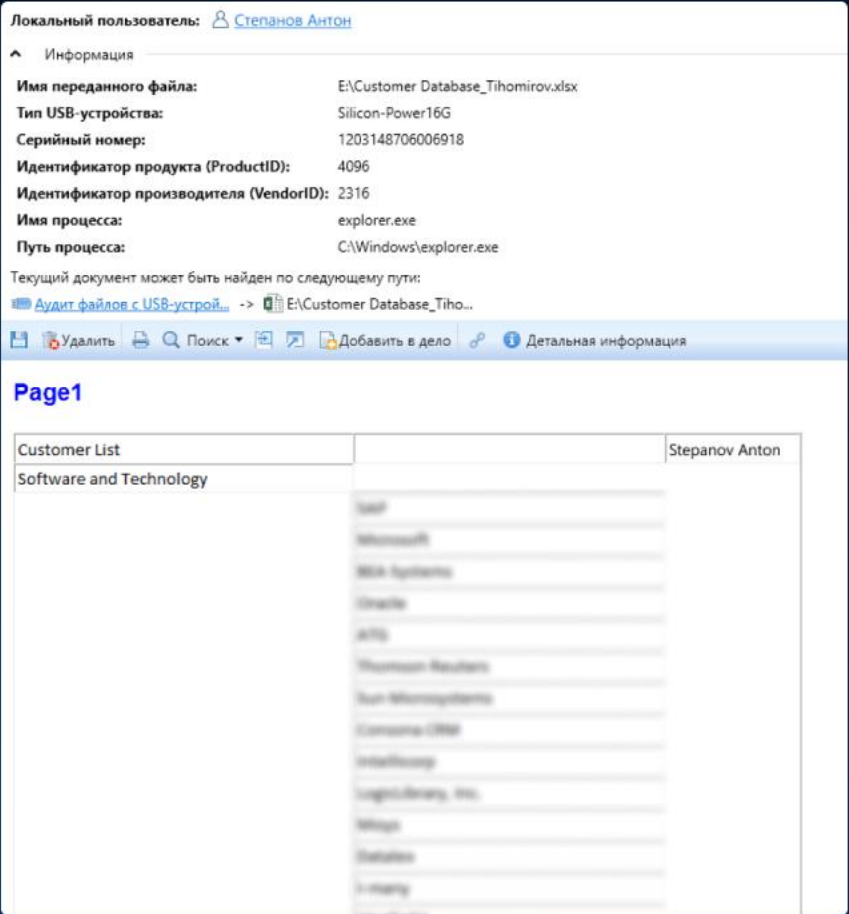
Комбинированный поиск



Активность пользователей



Агенты (Консоль Администратора)



Комбинированный поиск (Область поиска - почта, мессенджеры)

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



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.

Результат

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

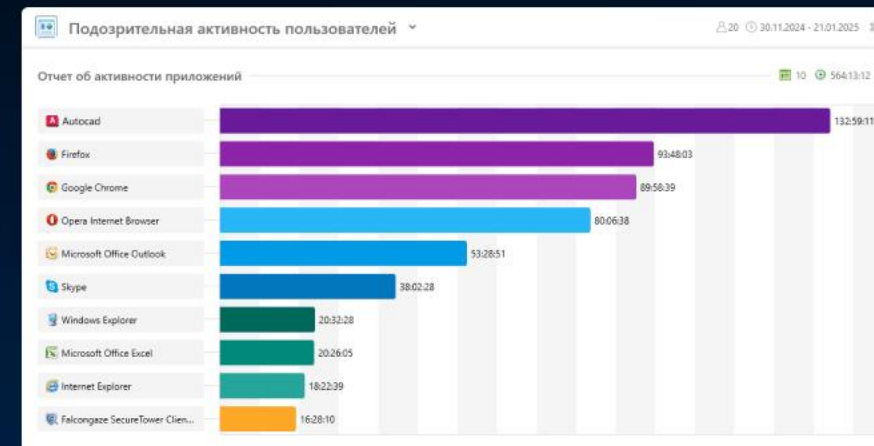
Модули, которые были использованы:



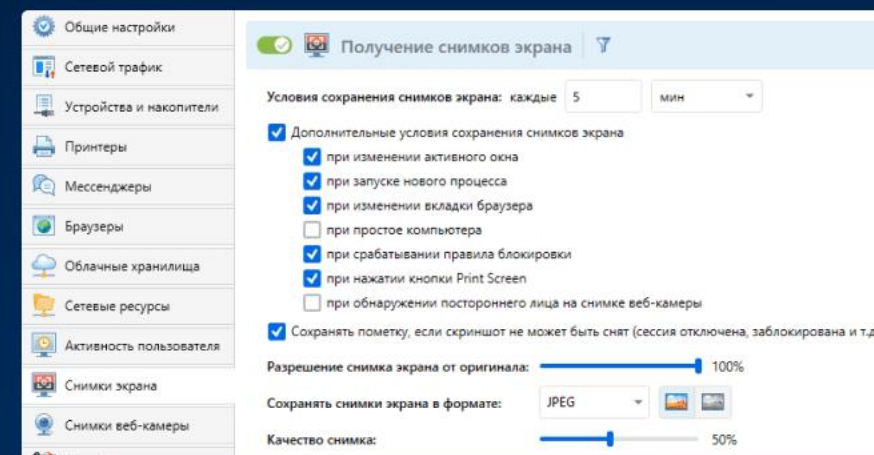
Политики безопасности



Отчеты



Модуль «Отчеты» (Отчет об активности пользователей)



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

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**

Сводный отчет по подозрительным пользователям

Пользователь	Браузер-активность: количество по...		Браузер-активность: время, провед...		Top посещенных сайтов		
	Σn	n	Σn	n	1 lll	2 lll	3 lll
Александр Тихонов	97	24.2	01:33:34	00:23:23	mail.google...	google.ru	habrahabr.ru
Владим Рогов	55	13.8	00:57:52	00:14:28	store.steamp...	yandex.ru	visualsvn.com
Александр Рогов	56	14	01:00:38	00:15:09	stackoverflo...	visualsvn.com	about
Александр Рогов	105	26.2	01:32:47	00:23:11	store.steamp...	yandex.ru	habrahabr.ru
Владим Рогов	83	20.8	01:17:11	00:19:17	stackoverflo...	google.ru	msdn.micros...
Владим Рогов	41	10.2	00:56:59	00:14:14	multitrn.ru	google.ru	linkedin.com
Александр Рогов	105	26.2	01:37:43	00:24:25	mail.google...	google.ru	habrahabr.ru
Александр Рогов	172	43	03:15:26	00:48:51	falcongaze.c...	multitrn.ru	mskit.ru
Александр Рогов	128	32	02:33:55	00:38:28	newtab	leprosorium.ru	youtube.com
Александр Рогов	96	24	01:30:54	00:22:43	store.steamp...	yandex.ru	adme.ru
Владим Рогов	51	12.8	00:56:19	00:14:04	stackoverflo...	djvu-soft.nar...	visualsvn.com
Александр Рогов	124	31	02:37:30	00:39:22	newtab	leprosorium.ru	youtube.com
Александр Рогов	104	26	01:35:38	00:23:54	mail.google...	google.ru	adme.ru
Александр Рогов	40	10	00:55:56	00:13:59	store.steamp...	yandex.ru	newtab
Владим Рогов	87	21.8	01:17:03	00:19:15	stackoverflo...	google.ru	b2bsky.ru
Александр Рогов	106	26.5	01:35:40	00:23:55	mail.google...	google.ru	top.rbc.ru
Александр Рогов	45	11.2	01:00:39	00:15:09	google.ru	translate.go...	lenta.ru
Александр Рогов	13	13	00:23:19	00:23:19	store.steamp...	yandex.ru	google.ru
Александр Рогов	59	14.8	00:58:49	00:14:42	stackoverflo...	djvu-soft.nar...	visualsvn.com
Всего (19)	1 567	21.1	27:37:52	00:22:42	store.steamp...	yandex.ru	newtab

Модуль «Отчеты» (Сводный отчет)

Нецелевое использование рабочего времени

Дата инцидента: 02.12.2024 8:42 Ответственное лицо: Administrator

Дело: Материалы расследования (5) Журнал событий

Добавить Сортировка Фильтры

#	Тип данных	Локальный пользователь	Удаленный пользователь	Перехвачено
1	Браузер-активность	Александр Рогов		30.11.2024 18:00:34
2	Браузер-активность	Владим Рогов		01.12.2024 16:44:24
3	Браузер-активность	Владим Рогов		02.12.2024 16:48:37
4	Браузер-активность	Владим Рогов		30.11.2024 16:35:11
5	Браузер-активность	Владим Рогов		02.12.2024 16:48:37

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

