StaffCop Enterprise 4.3

Программный комплекс для контроля информации,
действий пользователей и системных событий
на рабочих компьютерах

www.staffcop.ru

МОНИТОРИНГ. АНАЛИЗ. ОПОВЕЩЕНИЕ. БЛОКИРОВКА

опасной и непродуктивной деятельности сотрудников

Для бизнеса и государственных организаций от 5 до 25 000+ сотрудников

Программный комплекс для контроля информации, действий пользователей и системных событий на рабочих компьютерах

Раннее обнаружение угроз ИБ

Система имеет гибкую настройку фильтров и оповещений, поэтому возможную утечку или вторжение удаётся обнаружить на ранней стадии, чем существенно сократить последствия.

Учет рабочего времени

Мониторинг активности пользователя за ПК.
Учет фактически отработанного времени, опозданий, ранних уходов, прогулов и простоев.

Оценка продуктивности сотрудников

Разделение использование программ, посещения сайтов на продуктивные и непродуктивные.
Настройка для отдельных пользователей, групп и отделов. Сравнение показателей.

Мониторинг бизнес-процессов

Поиск «узких» мест, выявление блокирующих факторов и расследование причин их появления.
Анализ бизнес-процессов по KPI.

Расследование инцидентов

StaffCop — это машина времени! В любой момент можно вернуться назад и посмотреть, что делал тот или иной сотрудник в указанном промежутке времени.

Анализ поведения пользователей

Автоматический анализ появления аномалий.
Удобные средства статистической визуализации: тепловые диаграммы, граф и дерево взаимосвязей.

Удаленное администрирование

С уведомлением или без уведомления пользователя.
Удалённый захват управления ПК. Удобно работать IT-специалистам и службе ИБ.

Инвентаризация компьютеров

Полная картина использования программных продуктов и аппаратного обеспечения.
Интенсивность использования и архив состояний.

Удобно и функционально!

Мощная аналитика

Контентный анализ файлов, наглядные графики и диаграммы, графы коммуникаций, многомерные отчеты и многое другое...

Удобный веб-интерфейс

Просматривайте и управляйте системой из любимого браузера из любой точки интернета с любого компьютера.

Современные технологии

В основе лежит OLAP-технология обработки данных, которая позволяет строить многомерные отчеты «на лету» и обрабатывать огромные объемы данных за секунды.

Как работает StaffCop

StaffCop уникальное, полностью интегрированное решение которое предназначено для мониторинга действий сотрудников, потоков информации и событий системы с продвинутой системой аналитики, с возможностью выявления нелояльных сотрудников и предупреждения вредоносных действий.

- Помогает снизить риск утечки данных и потери репутации
- Позволяет увидеть ваши бизнес процессы в действии
- Обеспечивает прозрачность рабочего пространства
- Быстрая окупаемость и минимальные вложения
- Удобный веб-интерфейс
- Простая установка

Клиент-серверная архитектура

Подключение агентов и администраторов к серверу осуществляется по защищенному протоколу HTTPs. Поддерживается работа в любых инфраструктурах, включая NAT-трансляцию, VPN-каналы и другие варианты подключения. Благодаря этому может функционировать на удаленном компьютере, не находящемся в локальной сети компании.

Оффлайн режим — контроль, даже когда пользователь вне сети

Если у агента нет связи с сервером, он собирает информацию в локальную базу данных и передает ее на сервер при первой же возможности. Эта функция позволяет обеспечить постоянный контроль сотрудников, выходящих в интернет через временные каналы связи — мобильные 3G/4G-модемы, публичные Wi-Fi-подключения и т. п. Таким образом, в случае, например, отъезда сотрудника с рабочим ноутбуком в командировку контроль над его действиями не теряется, и мониторинг происходит в обычном порядке.

Комплекс StaffCop Enterprise состоит из двух частей: сервера и службы-агента.

Программа агент запускается на рабочих станциях сотрудников или терминальных серверах, с операционной системой Windows или GNU/Linux, собирает данные действий пользователя и события, передает их на центральный сервер, для обработки и визуализации.

Сбор данных
Собираются все события активности на компьютерах (конечных точках) для последующего анализа, оповещения и принятия решения.

Анализ
Автоматический и статистический анализ данных для выявления отклонений в поведении пользователей, выявления инцидентов, инсайдеров и нелояльных сотрудников.

Оповещение
Автоматическое оповещение о нарушении политик безопасности, опасной и непродуктивной деятельности сотрудников.

Отчеты
Разнообразные табличные и графические отчеты с возможностью периодической отправки по электронной почте. Используйте предустановленные отчеты или легко создавайте собственные с помощью мощного конструктора.

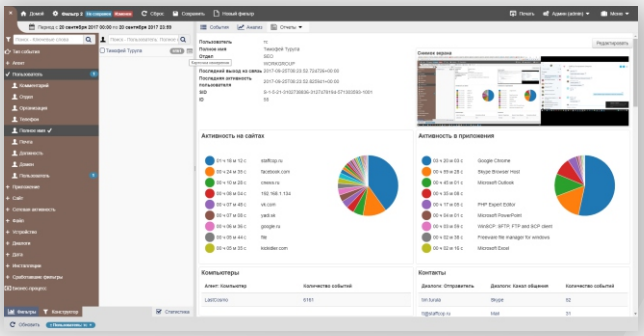
Блокировка
Блокировка запуска процессов и приложений, доступа к сайтам, съемным USB-носителям для повышения эффективности труда сотрудников и снижения рисков заражения вредоносным ПО.

Расследование
Поиск по всем данным и файлам с помощью фраз и регулярных выражений, корреляция событий. Техника «дрилл-даун» позволит находить данные, очищенные от информационного шума в несколько кликов.

Информационная безопасность

StaffCop построен на современных технологиях перехвата и анализа данных

В основе лежит технология OLAP, позволяющая обрабатывать большие массивы данных в онлайн режиме с огромной скоростью.



МОЩНАЯ АНАЛИТИКА

Поиск документов по цифровым отпечаткам
Контентный анализ документов
Сквозной поиск по словам и регулярным выражениям
Поддержка морфологии
OCR - распознавание текста на изображениях
Автоматический детектор аномалий поведения
Встроенные и пользовательские словари
Определение зашифрованных архивов
Поиск документов по цифровым отпечаткам
Многомерные интерактивные отчеты
Графы взаимосвязей событий
Тепловые диаграммы
Аналитические таблицы и графики

ОПОВЕЩЕНИЯ ОБ УГРОЗАХ

StaffCop может оповещать о нарушении политик безопасности в панели администратора и по электронной почте.

С помощью конструктора фильтров легко создавать всевозможные политики, соответствующие политикам безопасности вашей организации, и назначать оповещения при их срабатывании.

ПЕРЕХВАТ ВСЕХ КАНАЛОВ И СОБЫТИЙ

на рабочих станциях и терминальных серверах

Почтовые протоколы

IMAP, SMTP, MAPI, POP3 и их шифрованные аналоги. Контроль отправки сообщений и передачи файлов через веб-сервисы электронной почты.

Мессенджеры

Skype, ICQ, Jabber (XMPP), MSN и другие.
С помощью связки кейлоггер- приложение/сайт- скриншот можно отслеживать переписку любых мессенджеров, чатов и других коммуникаций через интернет.

Приложения

Факты установки и запуска приложений, продолжительность использования, скриншоты экрана при смене фокуса окна. Блокировка запуска процессов и приложений.

Файлы

Регистрация всех операций с файлами и папками, в том числе сетевыми. Создание теневых копий файлов отправляемых за пределы организации.

USB порты

Мониторинг операций со съемными носителями. Блокировка USB устройств по классам и HardwareID. Ограничение записи на USB и CD.

Печать на принтерах

Регистрация фактов печати: пользователь, время, компьютер, количество страниц и т.д. Создание теневых копий распечатываемых документов.

Сетевая активность

Регистрация сетевых подключений и контроль шифрованного трафика, посещения веб-сайтов, а также поисковые запросы пользователей.

SIP-телефония

Регистрация фактов и продолжительности звонков, перехват SMS-сообщений.

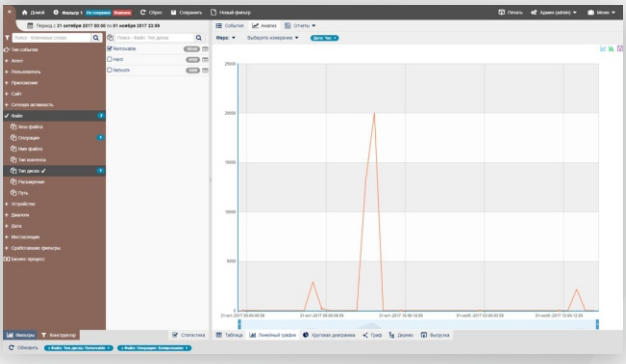
Аудио и видео регистрация

Запись окружения с микрофонов, видео рабочего стола, скриншоты экранов и снимки с веб-камеры.

Расследование инцидентов

StaffCop – машина времени!

Можно вернуться назад в любой момент и увидеть, что делал сотрудник в указанный момент времени и какие события привели к возможности инцидента.



Конструктор многомерных отчётов позволяет «на лету» получить необходимый набор данных. Поиск по ключевым словам и регулярным выражениям до минимума сократит время расследования инцидента, а функция записи окружения с микрофона компьютера позволит еще и услышать, что происходило в нужный момент.

Графы взаимосвязей

Наглядный просмотр коммуникаций сотрудников, их интенсивность. Схема миграции файлов внутри организации и передачи за ее пределы.

Графики выявления аномалий

Линейные, круговые, гистограммы и аналитические таблицы. Помогут представить данные в удобном виде.

Тепловые диаграммы

Удобны для определения интенсивности активности и событий сотрудников.

Карточки измерений

Сводные отчеты отображающие характеристики объекта и события с ним связанные. Карточки сотрудников, файлов, сайтов и т.д.

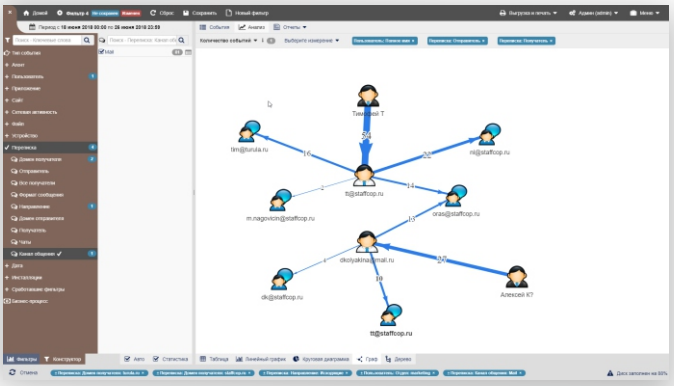
Экспорт и печать данных

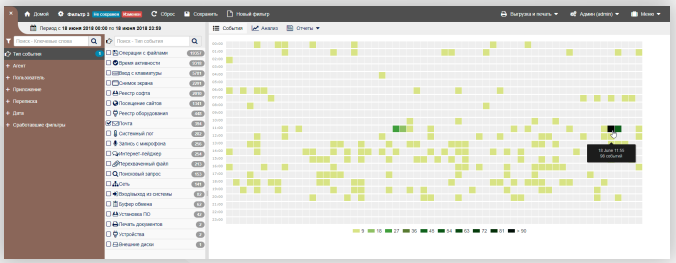
Отчеты и события можно выгрузить в PDF или в Excel.

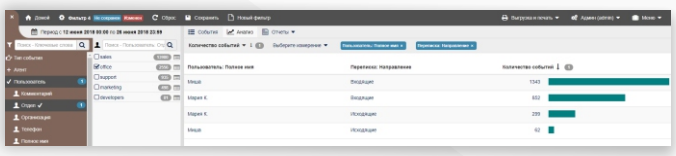
Быстро! Даже на больших данных.

Применение модели OLAP-куб делает возможным гибкий анализ данных: расследование инцидентов по цепочке, быстрый переход об общего к частному, составление аналитических отчетов по выбранным срезам данных.

Уникальное сочетание PostgreSQL и ClickHouse дает огромную скорость обработки данных. Не нужно ставить генерацию отчета на ночь, чтобы узнать, что там нет ничего нужного — расследуйте здесь и сейчас!







Контроль сотрудников на GNU/Linux

StaffCop работает на современных дистрибутивах, включая Ubuntu, Red Hat, Arch Linux и Astra Linux.

Позволяет вести мониторинг и анализировать действия пользователей на компьютерах под управлением как в оконной среде X-Windows, так и в терминальном режиме.

Регистрация входа в систему

Пользователи регистрируются системой при каждом входе и выходе. В лог попадают пользователи, входящие локально и удаленно, включая SSH-подключения.

Скриншоты экрана

Программа сохраняет снимки экрана пользователя по интервалу времени и переключению активного окна с фиксацией названия приложения и заголовка окна.

Файловые операции

StaffCop регистрирует операции с файлами: чтение, запись, удаление, создание и переименование. Создание теневых копий

Время активности в приложениях

Система регистрирует время работы пользователя в приложениях. Из собранных данных формируется отчет о продуктивности сотрудников по заданным критериям. Данные отчета сопоставляются со скриншотами по временным меткам. Возможен быстрый переход из графиков и таблиц к событиям.

Кейлоггер и регистрация bash-команд

StaffCop поддерживает перехват нажатий клавиш на уровне ядра для контроля терминала серверов, а так же перехват клавиатуры X-сессий.

Запись с микрофонов

Со встроенных и подключаемых микрофонов. Настройки позволяют задать шумовой порог начала записи, длину записываемых отрезков и уровень.

Регистрация USB-устройств

Флешки, принтеры и любые другие периферийные устройства попадают в лог. Администратор может проанализировать, где и когда подключались носители, отследить, в какие компьютеры подключались интересующие устройства.

История и время посещений веб-сайтов

Система регистрирует посещения веб-сайтов во вкладках браузеров Chrome, Firefox и браузеров на их основе. Кроме того, система вычисляет время, проведенное на веб-сайтах.

Фиксация фактов печати на принтере

Факты печати на принтере попадают в отчет системы с именами пользователей и названиями файлов. Пока без теневого копирования документа.

Мониторинг конфигурируемых лог-файлов

StaffCop Enterprise отслеживает изменения заданных лог-файлов, в том числе syslog. События создаются на каждое дополнение лог-файла.

Буфер обмена

Система перехватывает содержимое буфера обмена. Администратор просматривает перехваченные данные и сортирует при помощи различных фильтров.

StaffCop – российское решение и подойдет для импортозамещения

ASTRALINUX® special edition

Сертификат совместимости с операционной системой специального назначения Astra Linux Special Edition

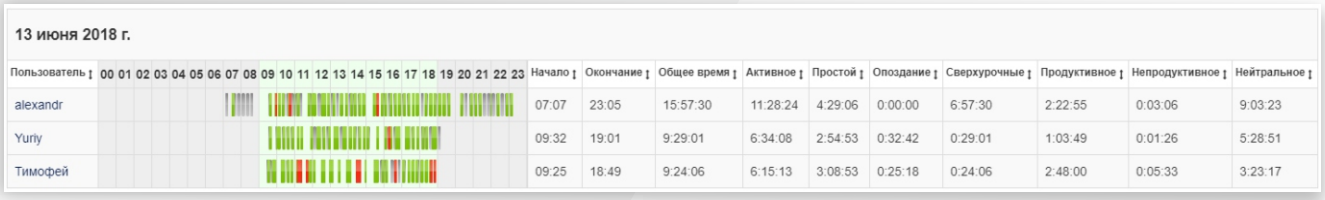
Минкомсвязь России

Внесен в единый реестр российского ПО за №3337

Контроль рабочего времени

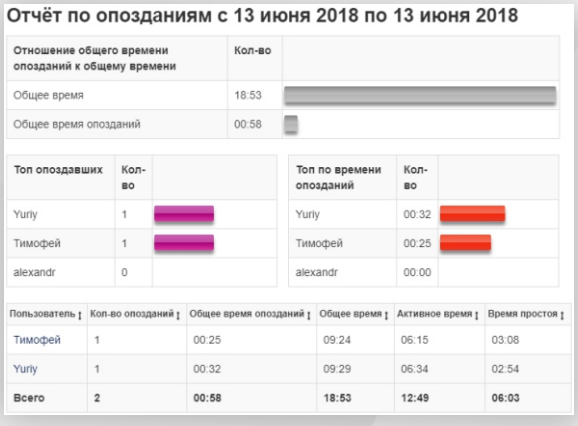
StaffCop не только фиксирует начало, окончание рабочего дня и перерывы, но и показывает детальную картину рабочего дня сотрудников

Уникальные алгоритмы определения активности позволяют максимально точно учитывать время в приложениях и на сайтах.



13 июня 2018 г.

Пользователь	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23	Начало	Окончание	Общее время	Активное	Простой	Опоздание	Сверхурочные	Продуктивное	Непродуктивное	Нейтральное
alexandr		07:07	23:05	15:57:30	11:28:24	4:29:06	0:00:00	6:57:30	2:22:55	0:03:06	9:03:23
Yuriy		09:32	19:01	9:29:01	6:34:08	2:54:53	0:32:42	0:29:01	1:03:49	0:01:26	5:28:51
Тимофей		09:25	18:49	9:24:06	6:15:13	3:08:53	0:25:18	0:24:06	2:48:00	0:05:33	3:23:17



Отчёт по опозданиям с 13 июня 2018 по 13 июня 2018

Отношение общего времени опозданий к общему времени	Кол-во
Общее время	18:53
Общее время опозданий	00:58

Топ опоздавших	Кол-во
Yuriy	1
Тимофей	1
alexandr	0

Топ по времени опозданий	Кол-во
Yuriy	00:32
Тимофей	00:25
alexandr	00:00

Пользователь	Кол-во опозданий	Общее время опозданий	Общее время	Активное время	Время простоя
Тимофей	1	00:25	09:24	06:15	03:08
Yuriy	1	00:32	09:29	06:34	02:54
Всего	**2**	**00:58**	**18:53**	**12:49**	**06:03**

Наглядная статистика:

- Опоздания
- Простои в работе
- Активное время за компьютером
- Продуктивное время
- Время затраченное на личные нужды
- Статистика по сотрудникам и отделам

После внедрения StaffCop продуктивность работы сотрудников увеличивается в среднем на
38%

Отчеты по электронной почте

по расписанию

StaffCop умеет отправлять вам каждое утро красочные отчеты в PDF по электронной почте.

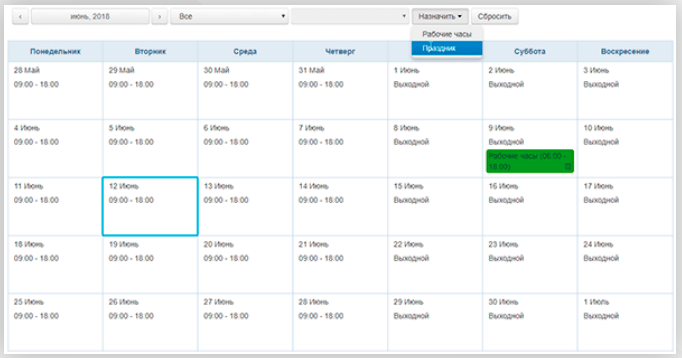
Это так же хорошо, как утренняя газета, только вместо уток и сплетен вы получаете достоверные факты.

Рабочее расписание для отделов и отдельных сотрудников

Не все сотрудники работают с 9 до 18 с понедельника до пятницы. Бывает, что кто-то уходит на больничный, а кто-то в отпуск.

В StaffCop можно настроить рабочее расписание с учетом особенностей графика сотрудников.

Это дает возможность получать максимально достоверную информацию по опозданиям и переработкам, и суммарную информацию по подразделениям.

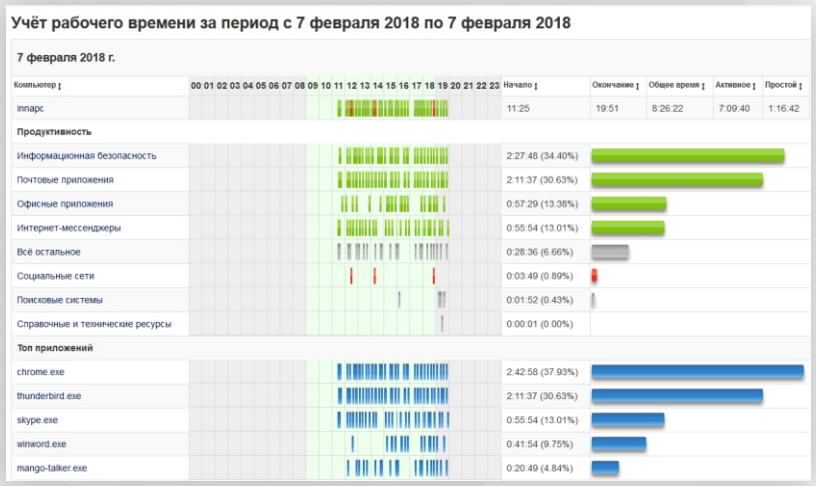


www.staffcop.ru

Анализ эффективности сотрудников

StaffCop покажет кто сколько времени тратит на работу, а сколько на личные цели.

Для разных категорий сотрудников можно настроить программы и сайты, которые требуются им для выполнения задач и которые «противопоказаны» к использованию.



Зеленые полоски — продуктивная деятельность.
Красные — непродуктивная или опасная.
Серые — нейтральная.

Нет полосок — не было деятельности.

Отвлекающие от работы программы и сайты могут быть заблокированы

Любые сайты или приложения, отвлекающие сотрудника от работы можно заблокировать, лично для сотрудника, для отдела или для всех.

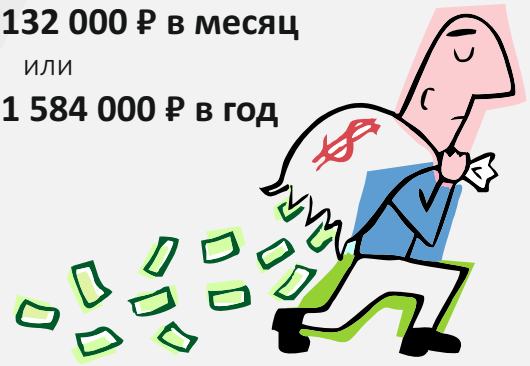
Немного статистики и вычислений

Мы опросили около 200 компаний, использующих StaffCop, суммарной численностью сотрудников более 4500 работающих за компьютерами. И составили картину распределения рабочего времени среднестатистического сотрудника в течение месяца:

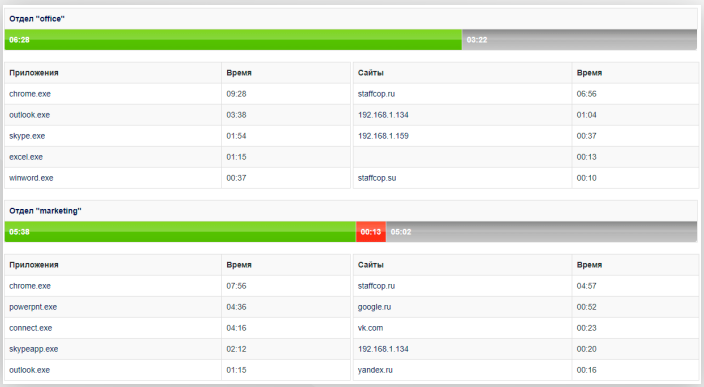
- 24% Заняты работой
- 37% Личные дела
- 7% Опоздания
- 13% Простой в работе

потери от оплачиваемой непродуктивной деятельности и опозданий 10 сотрудников, со средней заработной платой 30 000 ₽:

132 000 ₽ в месяц
или
1 584 000 ₽ в год



Суммарные отчеты по отделам



топ непродуктивности по отделам
продуктивное время по отделам
присутствие на рабочих местах
активное время по отделам

www.staffcop.ru

Удаленное администрирование и аудит IT

Мониторинг процессов и приложений, системных событий, подключение к удаленному рабочему столу делают StaffCop Enterprise незаменимым помощником IT-специалиста.

Вы сможете видеть кто и когда устанавливал, удалял или запускал программы, контролировать сетевые подключения, блокировать запуск «нежелательных» программ и сайтов.

Все данные консолидированы в одном месте,
больше не надо танцев с бубном, логами и прокси.

Блокировка сайтов и приложений

StaffCop делает возможным запретить каждой группе пользователей индивидуальный набор рабочих сайтов и приложений и заблокировать отвлекающие от работы.

Инвентаризация «железа» и «софта»

StaffCop собирает данные об устройствах и установленном программном обеспечении на компьютерах сотрудников. Дает возможность обнаружить пропажу или подмену оборудования, а также «запрещенные» программы.

Контроль и блокировка USB

StaffCop позволяет получить список всех программ установленных на компьютере, а так же список всех устройств компьютера с их идентификаторами.

Контроль установки приложений

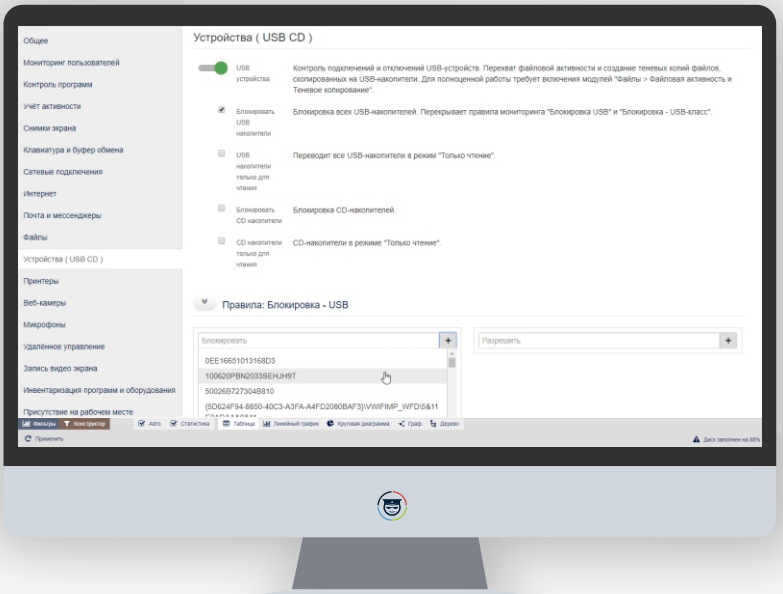
StaffCop позволяет получить список всех программ установленных на компьютере, а также список всех устройств компьютера с их идентификаторами.

Удаленное управление АРМ

С помощью StaffCop Enterprise можно просматривать действия сотрудников в онлайн-режиме и при необходимости получить управление без паролей и авторизации.

Сетевая активность

Позволяет определить по каким ip-адресам и портам, с помощью какого приложения производилось соединение.



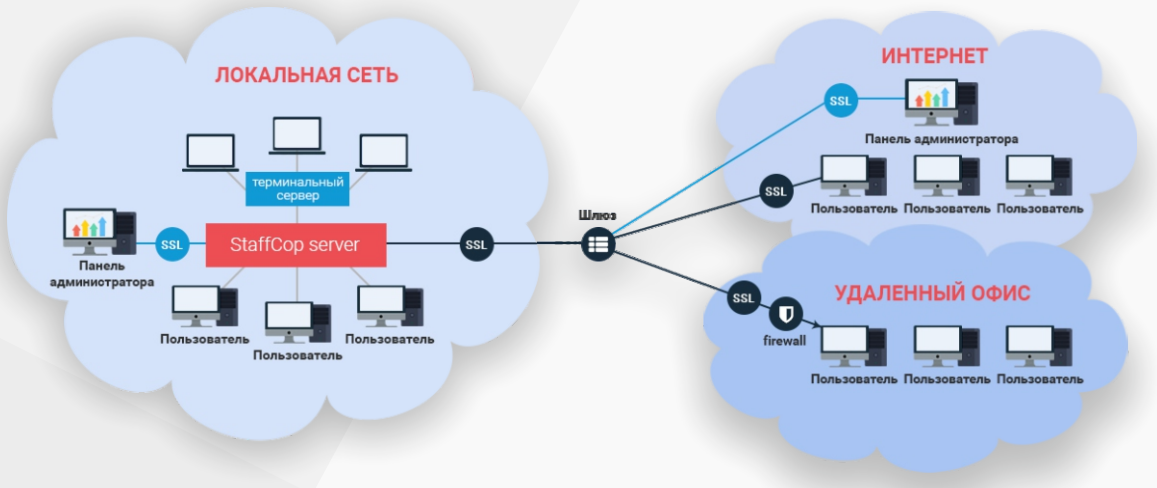
www.staffcop.ru

Архитектура StaffCop

Контроль компьютеров и терминальных серверов в локальных, распределенных и смешанных сетях любой сложности

В сетевых инфраструктурах обеспечивающих подключение от клиента к серверу через VPN, NAT и другие каналы

- Мониторинг рабочих станций в локальной сети
- Централизованный контроль удаленных офисов
- Контроль удаленных сотрудников



АГЕНТЫ МОНИТОРИНГА

Программа агент запускается на рабочих станциях или терминальных серверах, с операционной системой Windows или GNU/Linux, отслеживает действия пользователя и события на его компьютере, передает их на сервер, а также реализует различные блокировки и запреты доступа.

Агент StaffCop Enterprise может работать на удаленном компьютере, не находящемся в локальной сети компании.

СЕРВЕР

Серверная часть работает на Ubuntu Server 16.04 LTS amd64 и может быть установлена на физической, виртуальной машине или VDS\VPS сервере.

Для работы StaffCop требуется только один сервер предназначенный для сбора, анализа, обработки и просмотра информации об активности пользователей и перехваченных данных.

Поддерживаемые операционные системы

Windows:
Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 10.1,
Windows XP- с ограниченной функциональностью.

Терминальные серверы на Windows:
Windows 2008, Windows 2008 R2,
Windows 2012 R2, Windows 2016.

GNU/Linux:
Ubuntu, Debian, CenOS, Gentoo, Arch, Rosa, AstraLinux.

Можно установить на Windows

Специальный инсталлятор установит виртуальную машину и сервер StaffCop Enterprise.

Работает в системах виртуализации

WMWare, VirtualBox, Hyper-V и Proxmox

PostgreSQL в связке с ClickHouse

Использование OLAP технологии с двумя БД, позволяет ускорить построение отчетов и работу с системой

Обе базы данных — свободно распространяемые с открытым исходным кодом

Девять важных причин выбрать StaffCop

Многомерные аналитические отчеты и схемы коммуникаций и движения информации с возможностью перехода от общего к частному.

Мониторинг и управление рабочими местами из единого веб-интерфейса, возможность просто и безопасно организовать доступ из любой точки интернета.

Работа в любых сетевых инфраструктурах — подойдет для контроля распределенной филиальной сети, удаленных офисов и сотрудников.

Уникальные функции мониторинга рабочих станций и терминалов серверов под управлением GNU/Linux систем — расширяет возможности контроля.

Построено на решениях с открытым исходным кодом — не требуется приобретать дополнительные лицензии на серверную ОС и базы данных.

Быстрая работа на больших объемах данных за счет использования современных баз данных ClickHouse и PostgreSQL на технологии OLAP-кубов.

Подробная документация, оперативная и компетентная техническая поддержка. Команда проекта обеспечивает полноценное сопровождение с начального этапа тестирования.

Возможность доработки под требования, интеграции с другими системами и бизнес-процессами заказчика.

Минимальные требования к «железу», разумная стоимость и бессрочные лицензии, как результат — низкая стоимость приобретения, внедрения и эксплуатации

Пилотный проект

Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.

Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро

Развертывание пилотного проекта обычно занимает не более одного дня

Легко

Требуется минимум усилий и ресурсов для запуска StaffCop Enterprise

Комплексно

Вы сможете оценить сразу весь комплекс решаемых задач и принять правильное решение

www.staffcop.ru

Сделано в России

StaffCop Enterprise – полностью российское решение

Это позволяет использовать его на предприятиях в рамках политики импортозамещения.

Минкомсвязь России

StaffCop внесен в Единый реестр российского ПО за №3337
приказом Минкомсвязи России №212 от 28.04.2017

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Подана заявка на сертификацию на отсутствие НДВ по 4 уровню контроля и соответствию НПА по съемным машинным носителям информации по 4 классу защиты.

ASTRALINUX special edition

Работает в ОС Ubuntu, Red Hat, Arch Linux.
Имеет сертификат совместимости с операционной системой специального назначения Astra Linux Special Edition.

академпарк
Технопарк Новосибирского Академгородка

Резидент Технопарка Новосибирского Академгородка с 2012 года.
Имеет статус инновационной компании Академпарка.

О компании

Компания «Атом Безопасность» — российский разработчик IT-решений в области информационной безопасности и контроля действий персонала.

Более 10 лет мы разрабатываем программные решения для повышения эффективности работы и снижения рисков, связанных с внутренними угрозами информационной безопасности. Среди наших клиентов представители крупного, среднего и малого бизнеса, коммерческие предприятия и государственные службы.

Наша цель- помогать компаниям вести бизнес без страха за сохранность конфиденциальной информации.

Входит в ведущие ассоциации разработчиков

АРПП Отечественный Софт

ISDEF INDEPENDENT SOFTWARE DEVELOPERS FORUM

СибАкадемСофт

Постоянный участник мероприятий в области информационной безопасности

BISA

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

infosecurity