StaffCop Enterprise 4.3

для банков и финасового сектора

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

www.staffcop.ru

МОНИТОРИНГ. АНАЛИЗ. ОПОВЕЩЕНИЕ. БЛОКИРОВКА

опасной и непродуктивной деятельности сотрудников

Для обеспечения непрерывности бизнес-процессов и информационной безопасности в корпоративной среде банков и финансовых организаций

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.

СООТВЕТСТВИЕ ГОСТ Р 57580.1 – 2017

В рамках обеспечения соответствия ГОСТ Р 57580.1 – 2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» StaffCop закроет требования регуляторов:

- Выявление фактов использования несанкционированных учетных записей (уволенные сотрудники, подрядчики, прекратившие сотрудничество);
- Регистрация событий защиты информации связанные с действиями эксплуатационного персонала обладающего привилегированными правами.
- Контроль и выявление аномальной сетевой активности приложений.
- Контроль (регистрация) размещения, установки и запуска ПО на компьютерах пользователей.
- Блокировка запуска неразрешенного для использования ПО для групп пользователей в режиме «черных» и «белых» списков.
- Регистрация и контентный анализ информации, передаваемой по почтовым протоколам, в том числе вложенных документов.
- Регистрация фактов печати и контентный анализ файлов, передаваемых на печать.
- Ограничение использования или ограничение записи подключаемых USB-устройств по классам и идентификаторам в режиме «черных» и «белых» списков.
- Ограничение записи на CD-носители.
- Регистрация фактов подключения и отключения съемных USB устройств с указанием даты и времени, компьютера, учетной записи, класса устройства и его идентификатора.
- Теневые копии и контентный анализ информации, копируемой на съемные носители. Регистрация фактов создания файлов на съемных носителях.
- Регистрация операций, связанных с осуществлением доступа работниками к ресурсам Интернет.
- Регистрация удаления (стирания) информации с машинных носителей информации
- Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации. Оперативное оповещение групп реагирования об инцидентах информационной безопасности, автоматически выявленных с помощью мониторинга и анализа событий.

Минкомсвязь России

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

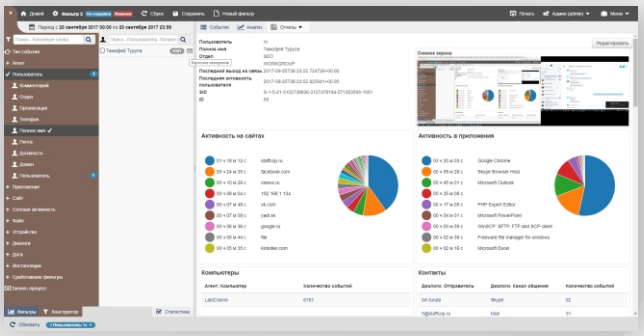
ФСТЭК России
Федеральная служба по техническому и экспортному контролю

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

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.

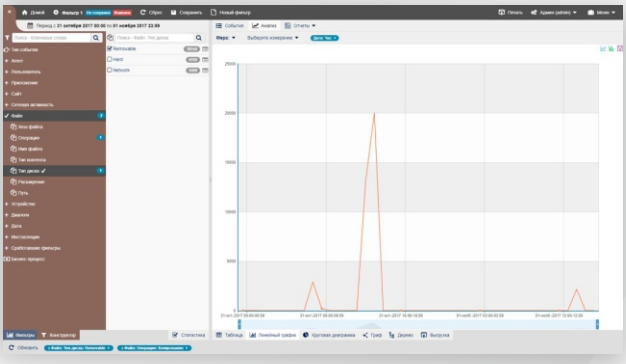
Аудио и видео регистрация

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.

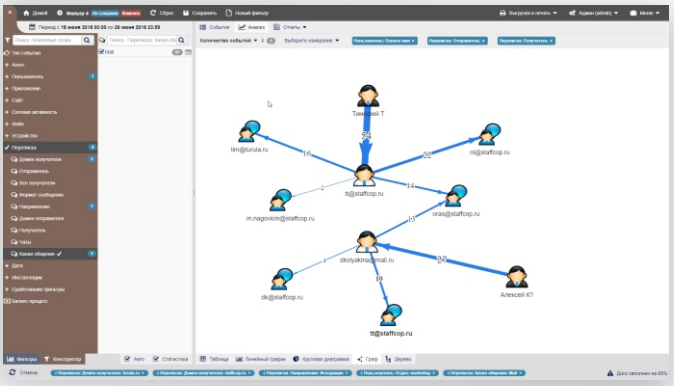
Экспорт и печать данных

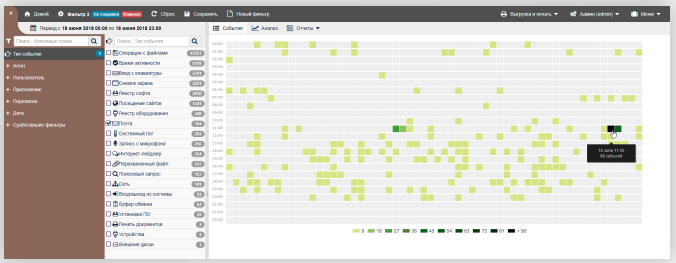
Отчеты и события можно выгрузить в PDF или в Excel.

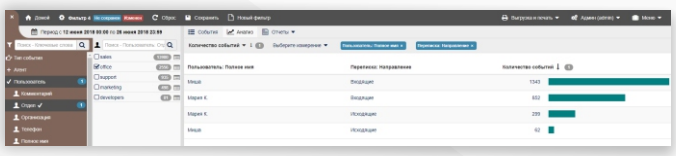
Быстро! Даже на больших данных.

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!







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

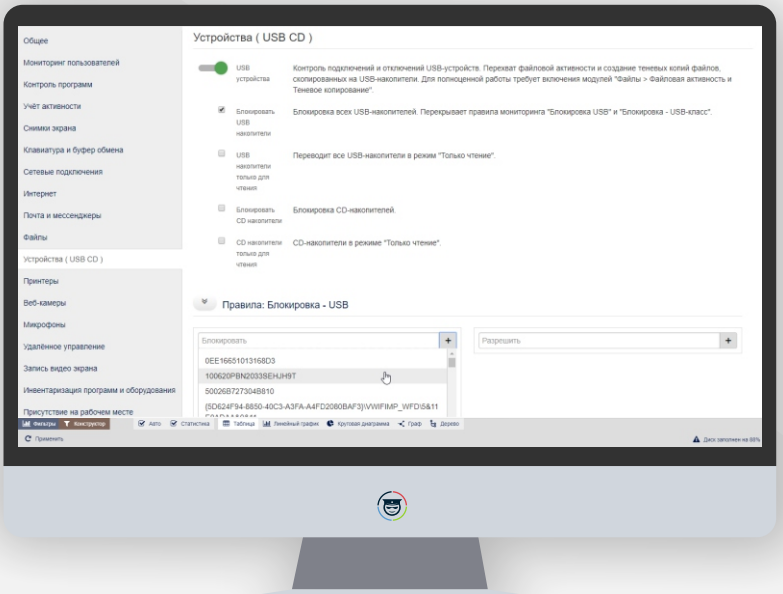
StaffCop позволяет получить список всех программ установленных на компьютере, а также список всех устройств компьютера с их идентификаторами.

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

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

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

ООО «Атом Безопасносность»

630090, г.Новосибирск,
Академгородок,
Институт математики
им. С.Л. Соболева СО РАН,
проспект академика Коптюга, д.4

www.staffcop.ru

Отдел продаж

+7 (499) 653-71-52

sales@staffcop.ru

Техническая поддержка

+7 (499) 638-28-09

support@staffcop.ru

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

Компания разрабатывает программы линейки StaffCop для повышения эффективности работы коммерческих предприятий и государственных служб, направленных на снижение рисков, связанных с внутренними угрозами информационной безопасности, обеспечивающих возможность мониторинга рабочих мест, событийного анализа, контроля рабочего времени и эффективности труда сотрудников организаций, оповещения об опасной и непродуктивной деятельности.

За многолетнюю историю существования клиентами стали более 10000 компаний из 26 стран мира.
На данный момент компания имеет широкую сеть партнёров в России и за рубежом.

В 2010 и 2016 году — продукты были признаны лучшими по версии журнала PC Magazine Russian Edition.

В 2017 году — продукт StaffCop Enterprise попал в ТОП-8 лучших продуктов контроля сотрудников на мировом рынке по версии журнала PCMag.com.

Компания является резидент Академпарка (Технопарка Новосибирского Академгородка) с 2012 года, имеет статус инновационной компании. Является действительным членом ведущих ассоциаций разработчиков программного обеспечения.

АРПП Отечественный Софт

ISDEF INDEPENDENT SOFTWARE DEVELOPERS FORUM

СибАкадемСофт

академпарк
Технопарк Новосибирского Академгородка

PC MAGAZINE RUSSIAN EDITION BEST 2010 SOFT

PC MAGAZINE RUSSIAN EDITION BEST 2016 SOFT

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00158 02/2016

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00181 12/2016

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

infosecurity

BISA