staffcop®

# Staffcop

## Возможости на GNU/Linux

Программный продукт для расследования и предотвращения инцидентов внутренней информационной безопасности.

staffcop.ru

## Сделано в России

Staffcop Enterprise – полностью российское решение. Это позволяет использовать его на предприятиях в рамках политики импортозамещения.

«Атом безопасность» внесена в Единый реестр IT-компаний Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации с регистрационным номером 9965 запись №95 от 15.03.2019 г.
Staffcop внесен в Единый реестр российского ПО под №8828.

Более 10 лет мы разрабатываем программные решения для расследования инцидентов внутренней информационной безопасности. Среди наших клиентов представители крупного, среднего и малого бизнеса, коммерческие предприятия и государственные службы.

## Для кого:

- Собственникам бизнеса
- IT специалистам
- ИБ специалистам
- HR

**10+**
Лет в информационной безопасности

**200 000+**
ПК под защитой Staffcop

**20+**
Отраслей бизнеса и промышленности, в которых мы работаем

**3 000+**
Клиентов в 40+ странах мира

Подтверждена совместимость:

base alt · РЕД ОПЕРАЦИОННАЯ СИСТЕМА · ASTRA LINUX · AlterOS

# Ввозможности на GNU/Linux

## Регистрация входа и выхода

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.

## Кейлоггер и регистрация bash-команд

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

## Буфер обмена

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

## Файловые операции

Staffcop регистрирует операции с файлами: чтение, запись, удаление, создание и переименование. Создание теневых копий при копировании на съемные носители.

## 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.

## Блокировка USB-устройств

Полная блокировка или ограничение записи на USB-устройства с целью обеспечения сохранности конфиденциальных данных организации и предупреждения заражения компьютеров вредоносным программным обеспечением.

## Блокировка сайтов

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

## Файловый сканер

Staffcop сканирует содержание файлов и извлекает контент из них.

## Перехват почты и мессенджеров

Извлечение писем по POP3, IMAP, SMTP протоколу, а также перехват популярных мессенджеров

## Администрирование

Индивидуальные правила можно применять к разным группам пользователей.

## Мониторинг лог-файлов

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

13

### Запись с микрофонов

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

14

### Контроль веб-камер

Поддержка просмотра видео с web-камер в режиме реального времени.

15

### DLP модуль

DLP модуль анализирует содержимое файлов, проверяет наличие цифровых меток и блокирует несанкционированный доступ по заданным параметрам.

16

### Централизованное обновление агента

Система позволяет централизовано обновить версию агента через интерфейс web консоли.

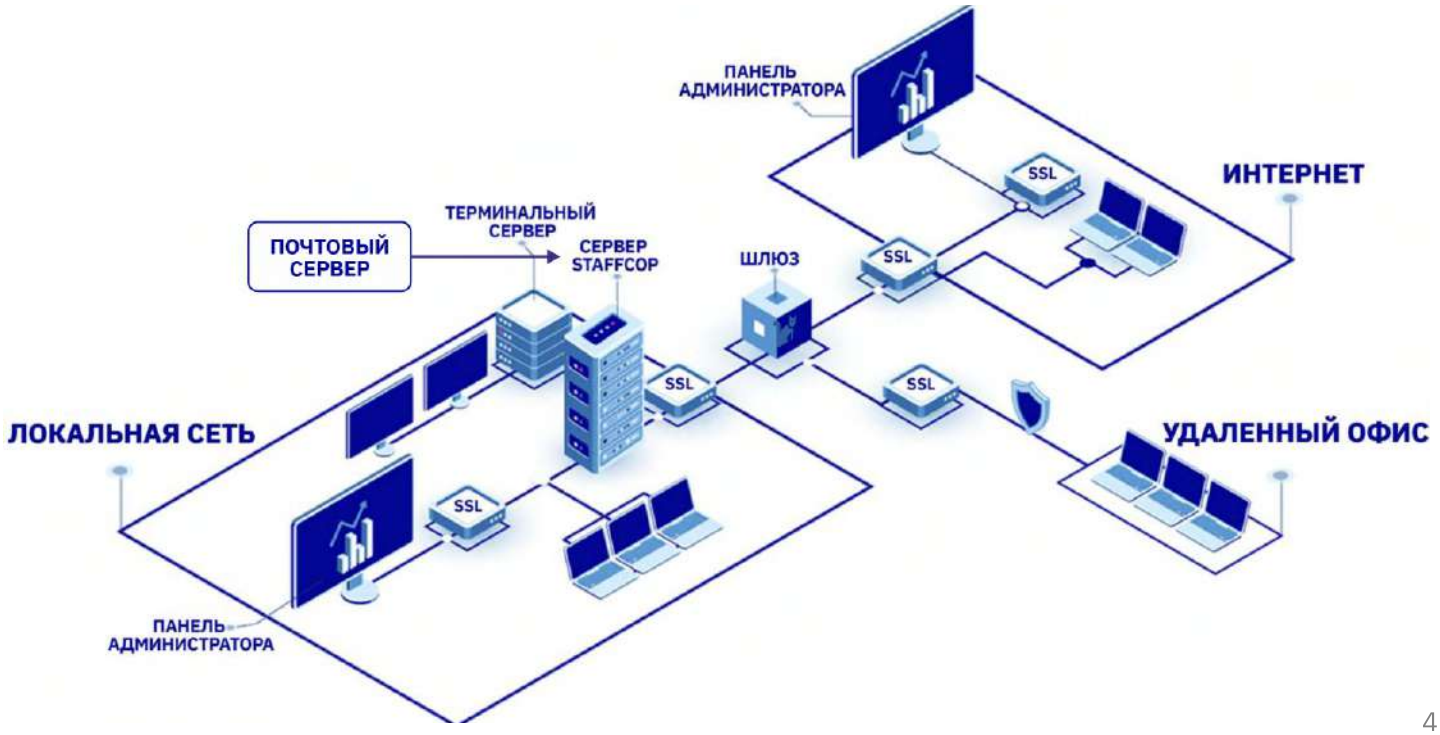
## Как работает Staffcop

Staffcop 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.

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

Программа запускается на рабочих станциях сотрудников или терминальных серверах, собирает данные действий пользователя и события, передает их на центральный сервер, для обработки и визуализации.

Если у агента нет связи с сервером, он собирает информацию в локальную базу данных и передает ее небольшими пакетами данных на сервер при первой же возможности.



## Пробуйте бесплатно

Дистрибутив и подробная документация на сайте staffcop.ru

### Быстро

Развертывание пилотного проекта обычно занимается не более одного дня.

### Легко

Требуется минимум усилий и ресурсов для запуска.

### Комплексно

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

**Полное техническое сопровождение на этапе тестирования!**

## Стоимость

### Бессрочная и срочная лицензия

Гибкая политика лицензирования.

### Бесплатные обновления

В течение 12 месяцев с момента приобретения.

### Бесплатная техподдержка

Оперативная и компетентная техподдержка в течение 1 года бесплатно.

## Политика лицензирования

### Что лицензируем

Лицензии на пользователей

Рабочая станция

Учетная запись

### Виды лицензий

| Срочная 3, 12, 24 мес. | Бессрочная |
|---|---|
| Тех. поддержка (стандарт) и обновления | |
| Включено в стоимость | Включено в стоимость на 1 год |

Агент мониторинга Staffcop имеет плавающий характер, предусмотрена возможность переносить агент на другие ПК без потери лицензии и архива данных. Установленный агент на рабочей станции осуществляет мониторинг активных учётных записей. При отсутствии учетных записей пользователей агент осуществляет мониторинг самой рабочей станции.

Бесплатная техническая поддержка и доступ к обновлениям программы предоставляются на срок лицензирования, но не более 12 месяцев с момента покупки. Тарифы на продление технической поддержки и доступа к обновлениям уточняйте у вашего менеджера.