



2021(2)



Даниил Бориславский
Руководитель аналитического
отдела
ООО Атом Безопасность
db@staffcop.ru





- Более 10 лет разработки приложений контроля сотрудников;
- Академгородок, Новосибирск, резиденты Технопарка и Сколково;
- Высокотехнологичная компания, ~50 сотрудников.
- Наша цель: «доступные решения задач информационной безопасности»
- Продано ~1300 серверных компонентов, ~ 66 000 АРМ за 2019-й год.
- Продано ~2200 серверных компонентов, ~ 171 000 АРМ за 2020-й год.





Система мониторинга для расследования инцидентов
и контроля работы сотрудников



учет рабочего
времени



эффективность
персонала



информационная
безопасность



расследование
инцидентов



удаленное
администрирование

2021

- Рост выручки (более 250 млн)
- Конференции offline и online
- Получаем ФСТЭК для новой версии
- Прошли сертификацию ФСБ
- Сотрудники: 42 -> 65+
- Рост международных продаж



Фичи 4.9 и 4.10

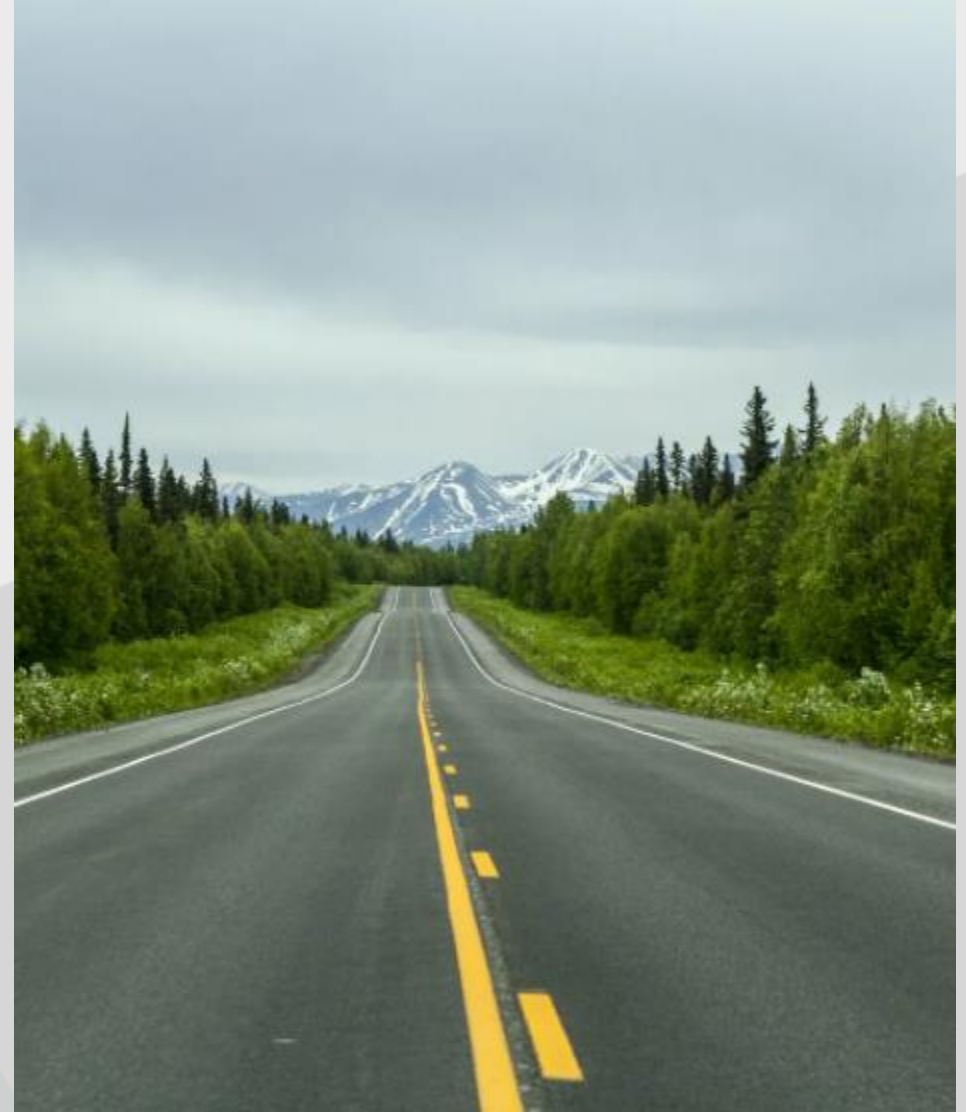
- Реакция на инцидент
- Новые возможности DLP модуля
- Блокировка USB по порогу
- Защита агента
- Linux агент
- Уведомления в телеграм
- Фермы распознавания
- Особый контроль для web-камер и видео рабочего стола
- Регулярные выражения в словарях
- Контроль рутокенов
- ETL модуль
- Контроль тех кто контролирует
- Интеграция со СКУД

... а лучше посмотрите вебинар

2022

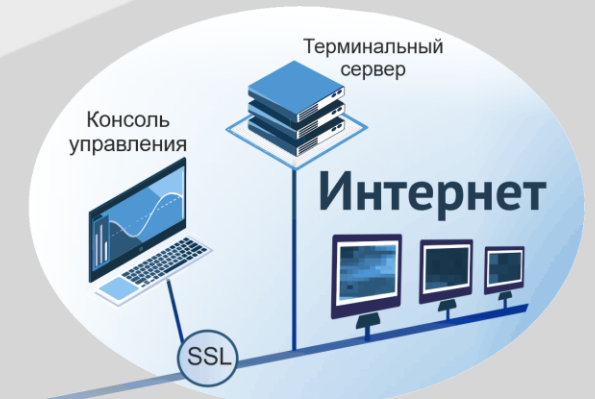
- Совместное развитие с СКБ-контур
- Расширение каналов перехвата
- Roadmap от клиентов
- Рост количества сотрудников в компании

... следите за новостями



Современные архитектурные решения

- Для работы сервера уже достаточно всего одной виртуальной машины
- Контроль ПК под управлением OS Windows, Linux, MacOS
- Система готова к сбору данных сразу после установки
- Удалённая установка агента
- 100 сотрудников <> 6CPU, 16RAM
- Локальные блокировки





- Нет дополнительных расходов за использование системы


Тотальный контроль действий за ПК


Инвентаризация «железа» и ПО


 Снимки с веб-камер

 Мониторинг посещенных сайтов и поисковых запросов

 Мониторинг действий в социальных сетях


 Контроль email-переписки


 Контроль USB и CD


 Мониторинг доступа к файлам




Сканирование хранящихся файлов

 Скриншоты и запись видео рабочего стола

 Подключение к рабочему столу

 Контроль печати

 Перехват сообщений в мессенджерах

 Кейлоггер

 Запись аудио с микрофона и колонок

Декодирование сервисов веб-почты и социальных сетей:

- mail.ru, yandex.ru, gmail.com...
- VK, FB, Одноклассники, LinkedIn...

Почтовые протоколы:

- SMTP / SMTPs
- IMAP
- POP3 / POP3s
- MS Exchange

Передача гипертекстовой информации и файлов:

- HTTP / HTTPS
- FTP / FTPs

Интернет-мессенджеры

- Skype
- ICQ, QIP, Jabber (XMPP)
- Mail.ru Agent
- Yahoo и другие

USB-порты

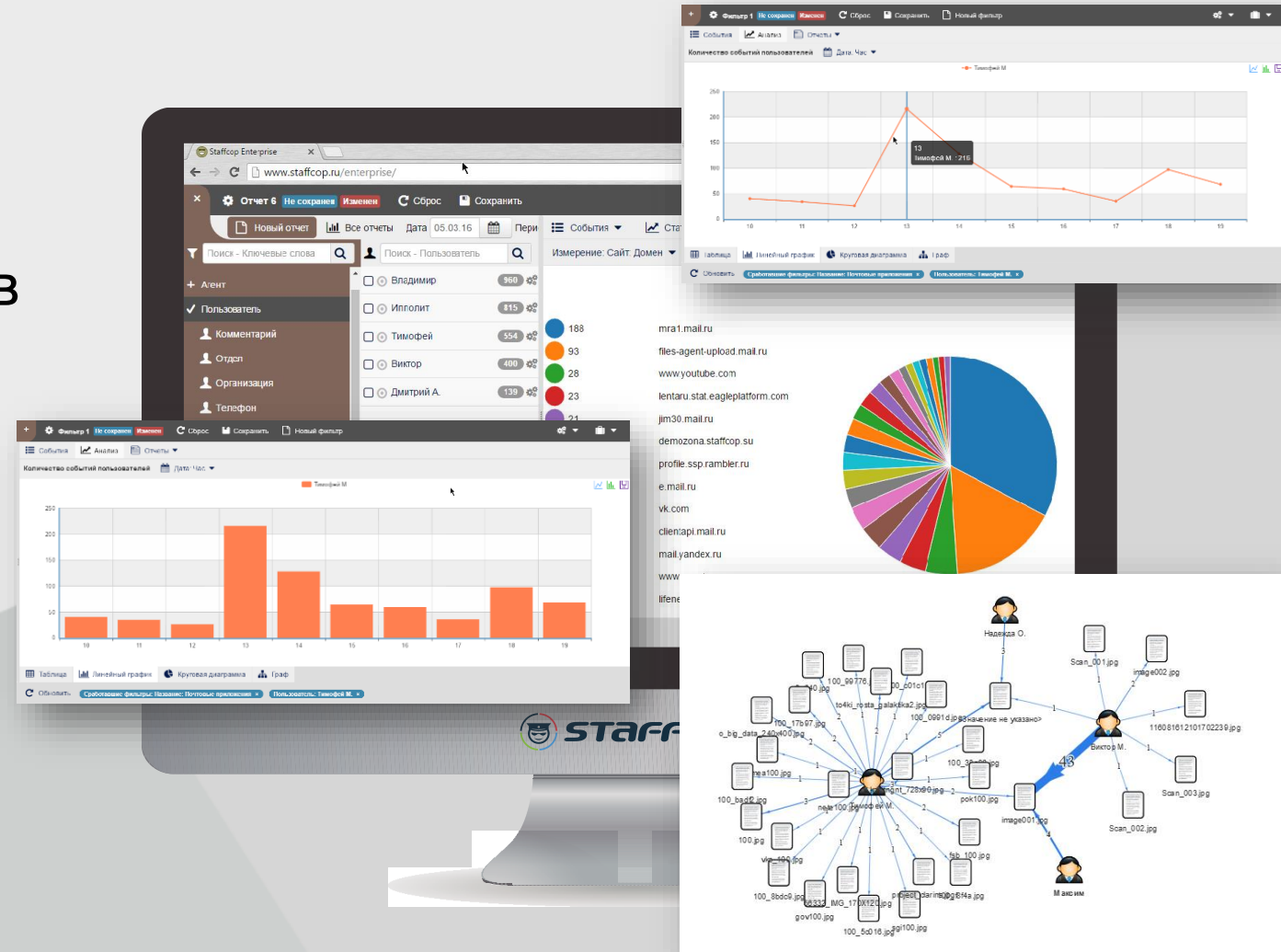
- контроль и блокировка

Теневое копирование файлов

- из электронной почты
- со съемных носителей
- переданных через интернет
- отправленных на печать

Расследование инцидентов ИБ

- Архив данных
- Конструктор многомерных отчетов
- Поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Система оповещений
- Гибкая система настройки фильтров



Учёт рабочего времени и его оценка

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 ↑
																								9:54:29	21:15:32	11:21:03	6:14:19	5:06:44
																								9:07:06	18:22:55	9:15:49	8:34:07	0:41:42
																								11:20:35	20:01:01	8:40:26	7:04:36	1:35:50
																								17:23:27	20:57:18	3:33:51	1:41:48	1:52:03
																								12:53:25	21:14:43	8:21:18	3:46:49	4:34:29
																								10:35:44	19:10:12	8:34:28	7:17:27	1:17:01
																								0:10:40	22:15:10	22:04:30	10:35:12	11:29:18
																								0:00:33	23:54:10	23:53:37	12:44:53	11:08:44
																								10:51:19	19:52:45	9:01:26	8:11:35	0:49:51
																								11:05:09	23:19:51	12:14:42	9:13:23	3:01:19

Дисциплина

Активность

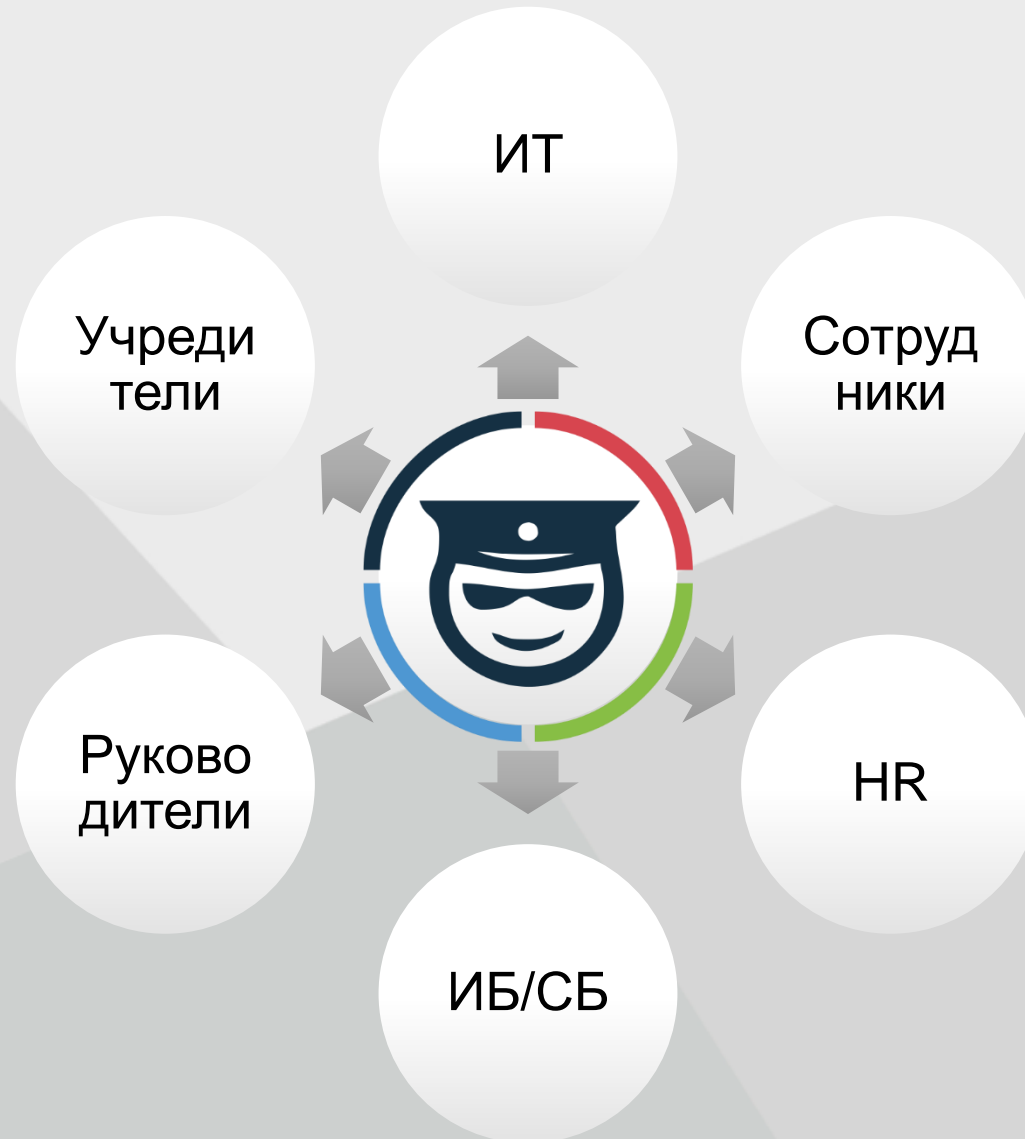
Продуктивность

Управление и администрирование



- Мониторинг
- Блокировки
- Инвентаризация ПО и «железа»
- Интеграция с SIEM
- Разные доступы для разных пользователей системы

Потребители



Преимущества Staffcop Enterprise



На opensource решениях, не требует дополнительного платного ПО.



Цена.



Входим в реестр отечественного ПО и имеет сертификат ФСТЭК.



Небольшие требования к ресурсам для сервера. Единая web-консоль.



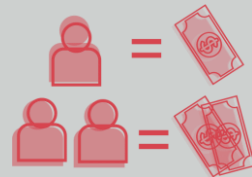
Настраиваемые отчёты и OLAP.



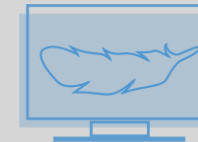
Не блокирует работу бизнеса.



Решает задачи разных подразделений



Единое решение и гибкая политика лицензирования.



Лёгкий и функциональный агент.

Аспекты эксплуатации



Правовые



Технические



Административные

Правовые аспекты внедрения

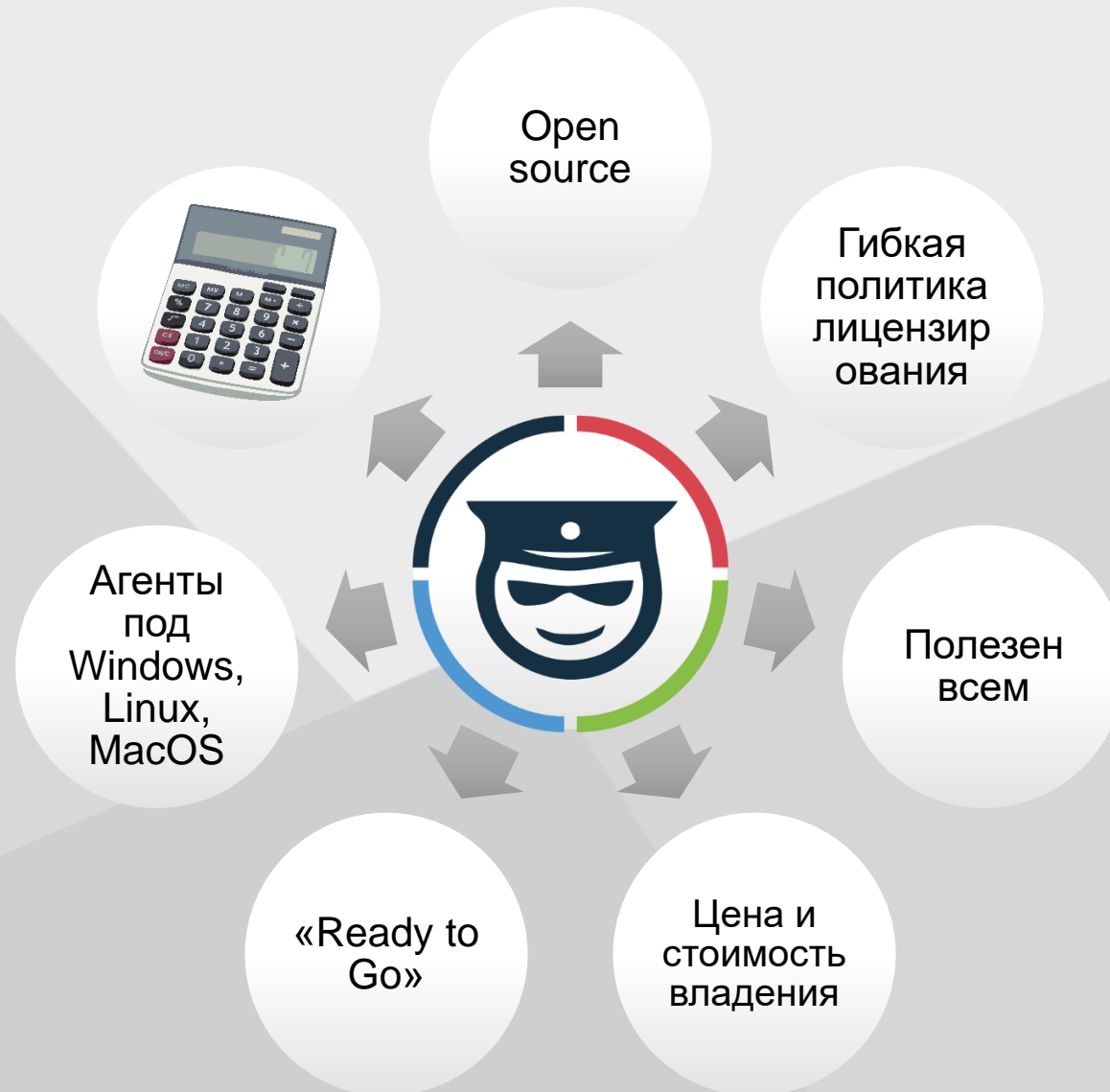
- **№149 ФЗ «Об информации, информационных технологиях и о защите информации».**
- **№98 ФЗ «О коммерческой тайне».**
- **№152 ФЗ «О защите персональных данных».**
- Определить и довести до работников правила использования средств хранения, обработки и передачи информации .
- Разработать и довести до работников регламент проведения мониторинга.
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации.
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору).

Технические аспекты внедрения и эксплуатации

- В дополнение к лицензиям на ПО могут потребоваться лицензии на OS и DataBase.
- Развёртывание и настройка системы.
- Система не должна мешать бизнесу работать.
- Не платите за то, что вам не нужно.
- Система должна быть полезной всем подразделениям.
- Система должна решать задачи поставленные бизнесом.
- Возможно, потребуется сертифицированная ФСТЭК версия.



Обоснование для внедрения



Политика лицензирования и стоимость

Количество компьютеров	Лицензия на 12 месяцев	Лицензия на 3 месяца
5–25	3 350 Р / 1 ПК	1 117 Р / 1 ПК
26–50	3 050 Р / 1 ПК	1 017 Р / 1 ПК
51–150	2 990 Р / 1 ПК	997 Р / 1 ПК
151–250	2 890 Р / 1 ПК	963 Р / 1 ПК
251–500	2 790 Р / 1 ПК	930 Р / 1 ПК
501–1000	2 690 Р / 1 ПК	897 Р / 1 ПК
1000+	2 590 Р / 1 ПК	863 Р / 1 ПК
Бессрочная лицензия – по запросу		

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



Благодарю за внимание!

Даниил Бориславский
Руководитель аналитического отдела
ООО Атом Безопасность

 +7(499)6382809 доб. 235
 db@staffcop.ru
 d.borislavskiy