Контроль информационных потоков и расследование инцидентов внутренней информационной безопасности

Бокал Артур

Менеджер по работе с партнерами

staffcop®

Расследование инцидентов внутренней безопасности

О компании

Единая консоль и многомерная архитектура данных позволяют расследовать любой инцидент за несколько кликов

11+ лет

Разработки приложений контроля сотрудников

Лучшее ПО для мониторинга сотрудников

По версии Forbes Advisor, 2023 г.

Импортонезависимый продукт. Российский разработчик

100 +

Сотрудников

200

Конференций, в которых мы приняли участие за 3 года

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

4 уровень доверия

АРПП Отечественный софт

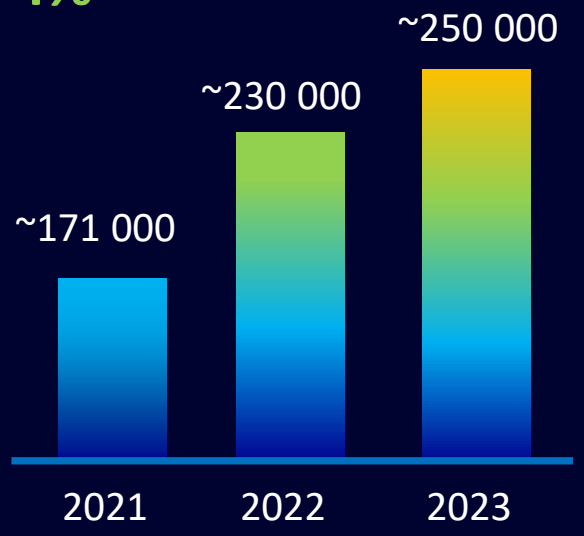
Минцифры России

Sk Участник

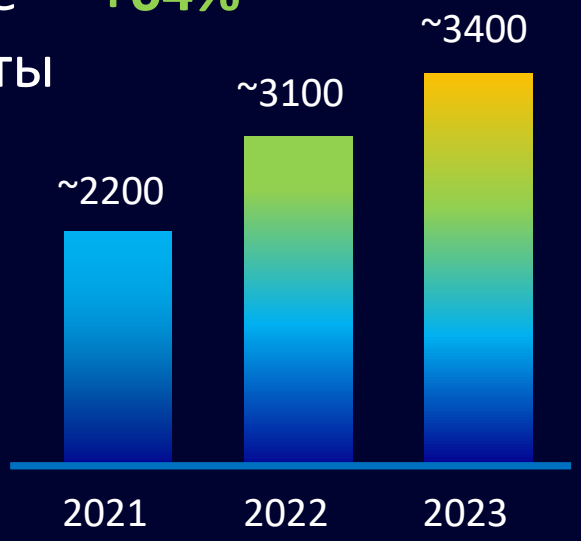
академпарк

О компании

ARM **+74%**



Серверные компоненты **+64%**



Клиенты:

20+ клиентов из Топ 100 Forbes

ЛУКОЙЛ · НЦВ Миль и Камов Холдинг вертолеты России · Ростех · ДОМ.РФ БАНК

Расследование инцидентов. Сбор доказательной базы

Утечка информации. Потеря данных

Риски, связанные с удаленной работой

Дисциплина сотрудников

Предупреждение опасных действий и мошеннических схем сотрудников

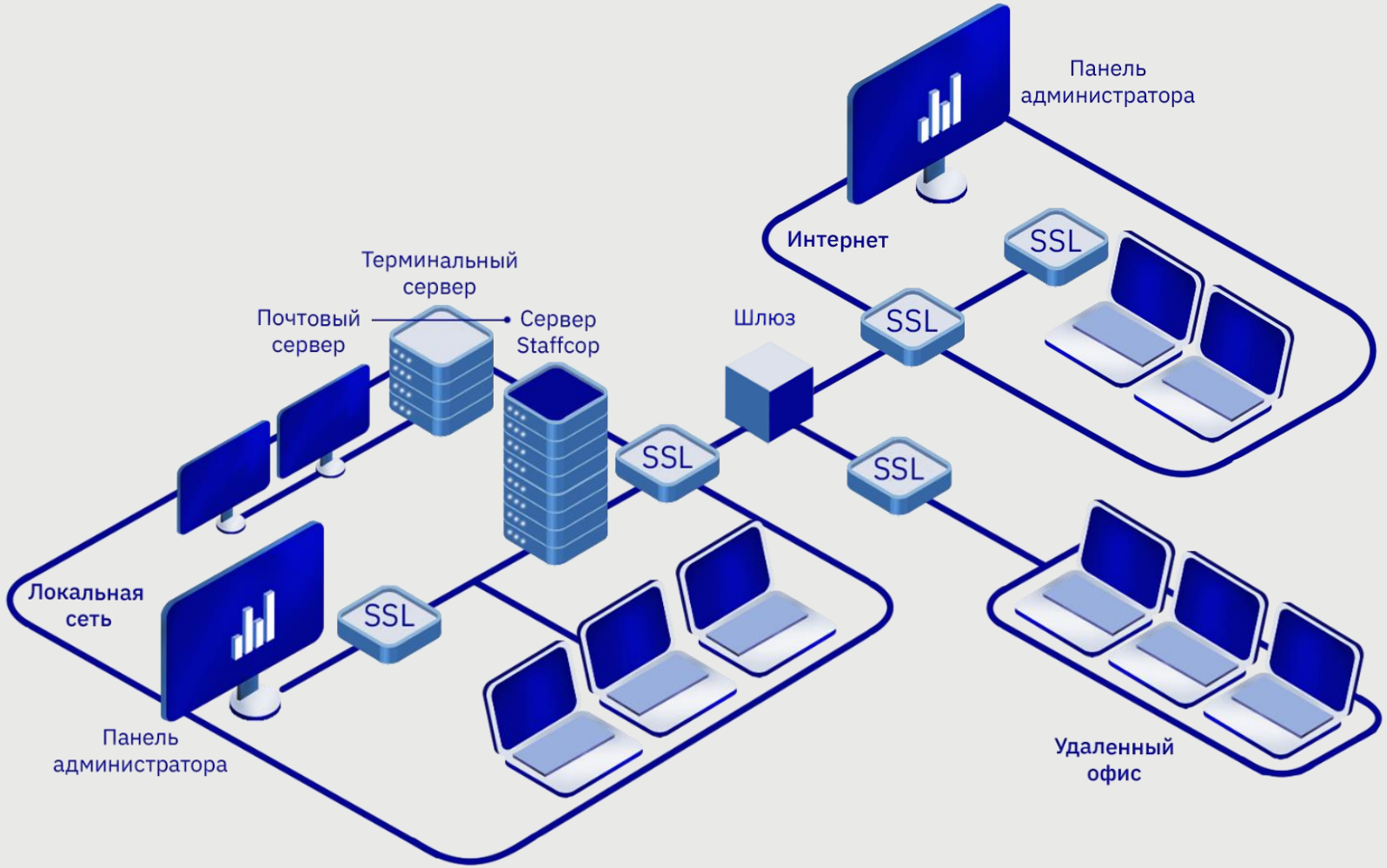
Контроль периферийного оборудования и ПО

Возможность сбора доказательной базы

staffcop

Современные архитектурные решения

- Единая веб-консоль
- 100 ПК <=> 6 CPU, 32 RAM
  1000 ПК <=> 12 CPU, 96 RAM
- Для работы достаточно одного виртуального сервера
- Агент для Windows, Linux, macOS
- Минимальные требования к железу
- Импортонезависимое ПО
- Масштабируемая архитектура
- OLAP технология хранения данных



Использование отечественного и независимого ПО

staffcop

Технологии сервера:

open source initiative

ASTRA LINUX®

ClickHouse

PostgreSQL

OS рабочих ПК и АРМ:

base alt

ROSA

ASTRA LINUX®

РЕДОС

Компоненты, не требующие лицензирования и покупки

staffcop

Основные функции

Действия пользователей

- Снимки с web камеры
- Скриншоты и запись видео с рабочего стола
- Мониторинг посещенных сайтов
- Контроль печати
- Мониторинг действий в социальных сетях
- Запись аудио с микрофона и колонок

Документы и файлы

- Контроль почты
- Перехват мессенджеров
- Мониторинг доступа к файлам

Действия системы

- Удаленное управление
- Контроль съемных носителей
- Мониторинг доступа к файлам

Решаемые задачи

Информационная безопасность

- Раннее обнаружение угроз ИБ
- Расследование инцидентов
- Анализ поведения пользователей

Эффективность работы персонала

- Оценка продуктивности сотрудников
- Мониторинг бизнес – процессов
- Учет рабочего времени

Администрирование рабочих мест

- Удаленное администрирование
- Инвентаризация компьютеров
- Индексирование файлов на ПК

Для кого?

Собственников бизнеса

IT специалистов

ИБ специалистов

Сотрудников HR

Собственникам бизнеса

ИБ специалистам

staffcop

Расследование инцидентов ИБ

01 Система оповещений

02 Гибкая система настройки фильтров

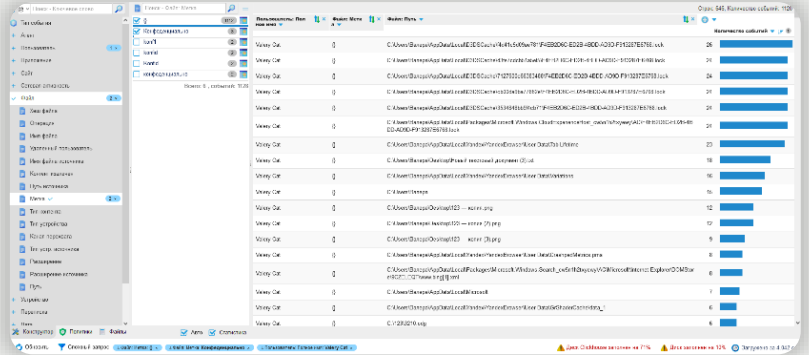
03 Графы взаимосвязей

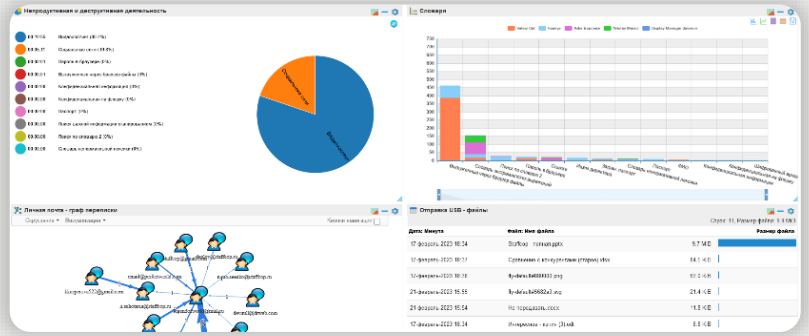
04 Метки для файлов

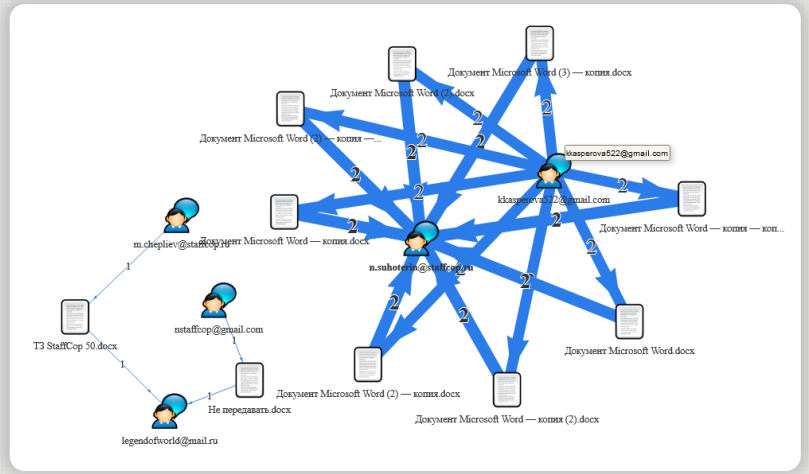
05 Изменение конфигурации контроля при наступлении определённого события

06 Защита от массового копирования

07 Нейронная сеть распознавания изображений







Собственникам бизнеса

IT специалистам

Сотрудникам HR

ИБ специалистам

staffcop

Аналитические возможности

01 Архив данных

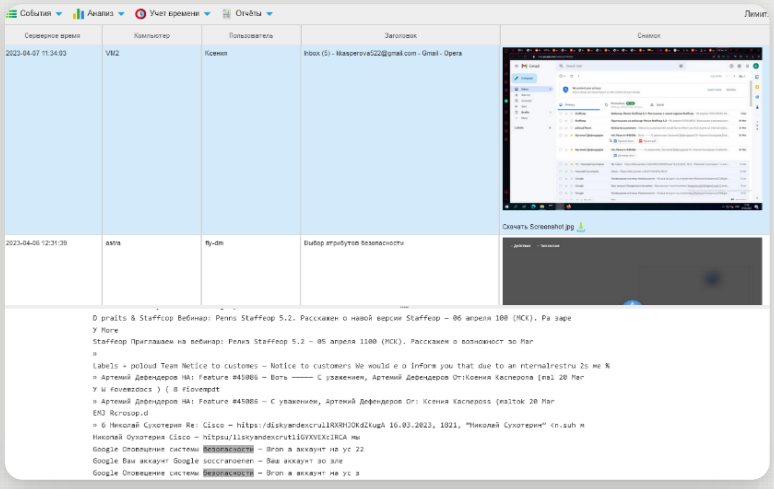
02 Поиск по словам и регулярным выражениям

03 Синхронизация данных с AD

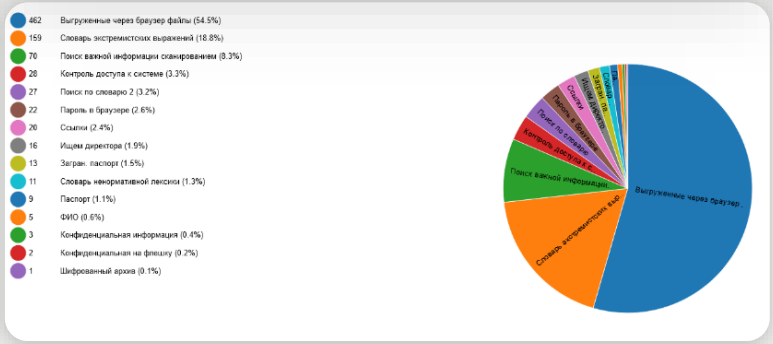
04 Конструктор многомерных отчетов

05 Множество графов и диаграмм

06 Speech-to-text



Astra Воронеж	Вход/выход из системы	6
Astra Воронеж	Буфер обмена	47
Astra Воронеж	Устройства	67
Astra Воронеж	Внешние диски	16
Astra Воронеж	Операции с файлами	41289
Astra Воронеж	Реестр оборудования	1001
Astra Воронеж	Реестр софта	8660
Astra Воронеж	Поисковый запрос	15
Astra Воронеж	Видео рабочего стола	7
Astra Воронеж	Терминал linux	4
Astra Воронеж	Линукс лог	7
Astra Воронеж	Время активности	1343



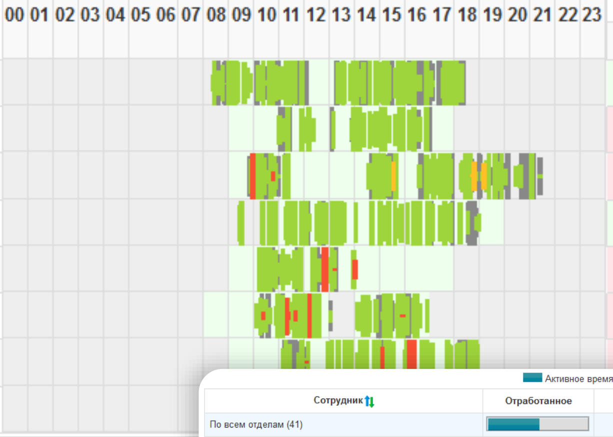
Собственникам бизнеса

Сотрудникам HR

staffcop

Учет рабочего времени и его оценка

Заняты работой	Личные дела	Опоздания	Простой в работе	Прочее
24%	37%	7%	13%	19%



Начало		Окончание		Общее время		Дисциплина		Деятельность		Продуктивность		
факт	распис	факт	распис	факт	план	сверх	опозд	актив	неактив	прод	непрод	нейтр
8:15:37	9:00:00	18:14:14	18:00:00	9:58:37	9:00:00	0:58:37	0:00:00	8:13:51	1:44:46	6:33:05	0:00:00	1:39:14
10:54:37	9:00:00	16:58:13	18:00:00	6:03:36	9:00:00	0:00:00	1:54:37	3:51:18	2:12:18	2:55:38	0:00:00	0:55:06
9:43:44	9:00:00	21:21:54	18:00:00	11:38:10	9:00:00	2:38:10	0:43:44	6:10:55	5:27:15	4:04:54	0:02:34	2:00:34
9:23:08	11:00:00	18:51:29	20:00:00	9:28:21	7:00:00	2:28:21	0:00:00	2:58:42	6:29:39	2:41:37	0:00:00	0:16:25
10:06:09	9:00:00	13:55:35	18:00:00	3:49:26	9:00:00	0:00:00	1:06:09	2:25:09	1:24:17	2:01:09	0:04:26	0:18:46
10:01:37	8:00:00	16:59:26	17:00:00	5:57:49	8:00:00	0:00:00	2:01:37	4:34:39	1:23:10	3:42:56	0:05:08	0:45:21
11:03:19	9:00:00	18:53:42	18:00:00	7:50:23	9:00:00	0:00:00	2:03:19	4:21:41	3:28:42	3:15:12	0:13:09	0:52:29
						0:00:00	0:33:01	5:24:09	2:17:14	3:58:46	0:00:00	1:22:49

Активное время / Неактивное время / Плановое время

Сотрудник	Отработанное	Активное	Переработка	Недоработка	Отсутствие	Плановое
По всем отделам (41)		942:40:03 (51,1 %)		901:19:57 (48,9 %)	131:00:00	1844:00:00
		48:48:27 (54,2 %)		41:11:33 (45,8 %)	9:00:00	90:00:00
		180:45:43 (50,2 %)		179:14:17 (49,8 %)	36:00:00	360:00:00
		9:33:24 (21,2 %)		35:26:36 (78,8 %)	9:00:00	45:00:00
		22:59:53 (51,1 %)		22:00:07 (48,9 %)	9:00:00	45:00:00
		27:24:02 (60,9 %)		17:35:58 (39,1 %)		45:00:00
		21:05:56 (46,9 %)		23:54:04 (53,1 %)		45:00:00
		30:15:07 (67,2 %)		14:44:53 (32,8 %)		45:00:00
		20:11:11 (44,9 %)		24:48:49 (55,1 %)	9:00:00	45:00:00
		19:43:25 (43,8 %)		25:16:35 (56,2 %)		45:00:00
		29:32:45 (65,7 %)		15:27:15 (34,3 %)	9:00:00	45:00:00
		44:11:25 (49,1 %)		45:48:35 (50,9 %)	9:00:00	90:00:00
		291:49:58 (54,4 %)		244:10:02 (45,6 %)	54:00:00	536:00:00
		60:42:35 (45,0 %)		74:17:25 (55,0 %)		135:00:00
		44:58:24 (99,9 %)		0:01:36 (0,1 %)		45:00:00
		63:54:27 (47,7 %)		70:05:33 (52,3 %)	9:00:00	134:00:00
		9:34:50 (19,6 %)		39:25:10 (80,4 %)	14:00:00	49:00:00
		106:43:11 (47,4 %)		118:16:49 (52,6 %)		225:00:00
		91:11:03 (50,7 %)		88:48:57 (49,3 %)		180:00:00

IT специалистам

ИБ специалистам

staffcop

Администрирование

01 Мониторинг аномальной активности

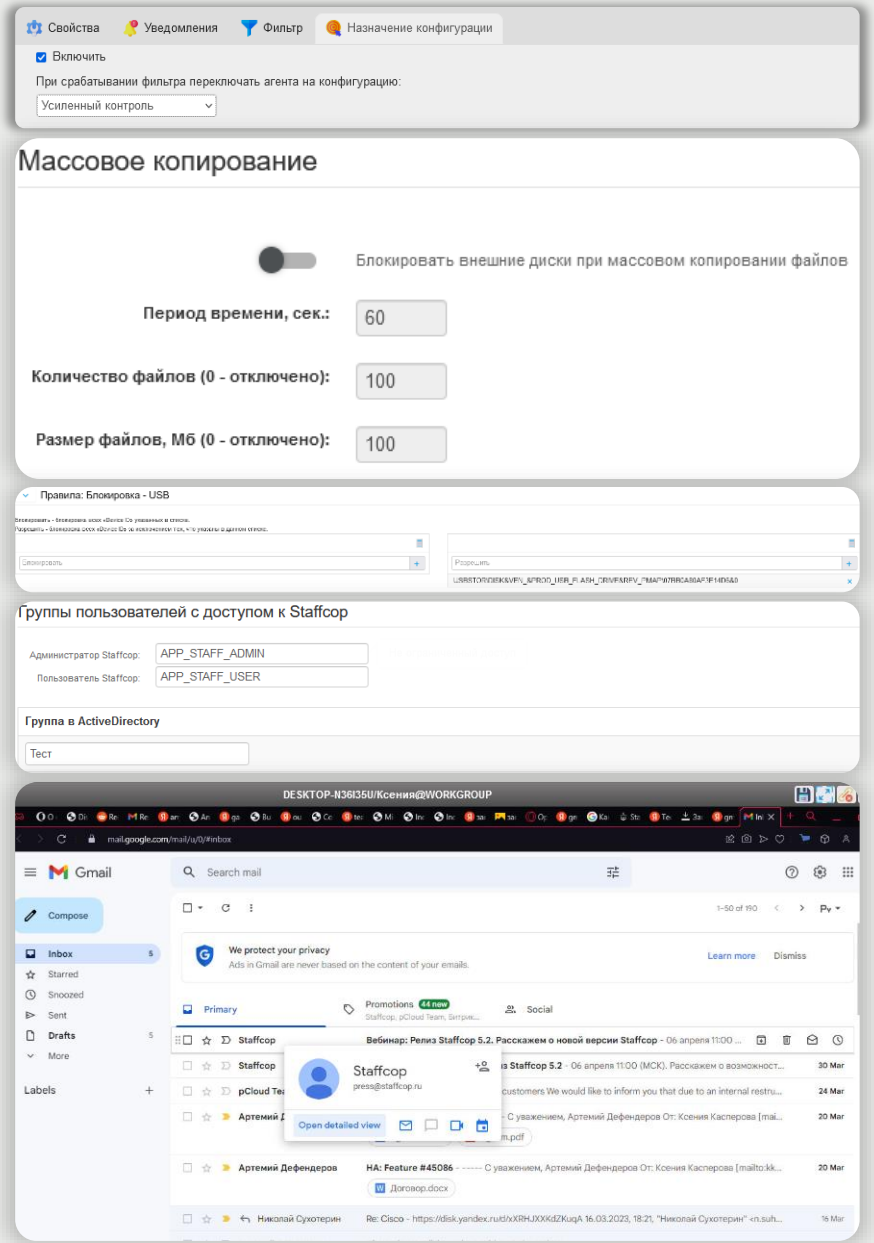
02 Блокировки съемных носителей

03 Инвентаризация ПО и «железа»

04 Удаленное наблюдение за АРМ и перехват управления

05 Интеграция с SIEM, AD, 1С, СКУД и другими системами ИБ и ИТ

06 Разные доступы для разных пользователей системы



staffcop

Если у вас уже есть DLP решения

Эшелонированная защита

На одной группе риска DLP. На другой - Staffcop

DLP на шлюзе.
Staffcop на end point

Оптимизируйте бюджет защиты ИБ

Обеспечим защиту ваших филиалов

Тестируйте уже сейчас!

Полное техническое сопровождение на этапе тестирования!

staffcop®

Быстро

Развертывание пилотного проекта обычно занимает 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

Бесплатный аудит

Позволит вскрыть точки роста в Вашей системе ИБ

staffcop

Аспекты внедрения

Этика внедрения

Технологические вопросы

Юридические вопросы

staffcop®

Преимущества Staffcop Enterprise

Кроссплатформенный

Быстрый и легкий

Простое и доступное лицензирование

Импортонезависимый

Качественная техническая поддержка

Индивидуальный подход, закрепленный менеджер

Расширенный пилот с полноценным функционалом

Доступ к регулярным обновлениям

Спасибо за внимание!

«За безопасность необходимо платить, а за ее отсутствие - расплачиваться»

/ Уинстон Черчилль /

Бокал Артур

Менеджер по работе с партнерами

staffcop®

Расследование инцидентов внутренней безопасности

staffcop.ru

Telegram