IRM: АКТУАЛЬНОСТЬ РАССЛЕДОВАНИЯ

Юрий Драченин

Заместитель генерального директора

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

100 +

Сотрудников

200 +

Конференций, в которых мы приняли участие за 3 года

Лучшее ПО для мониторинга сотрудников

По версии Forbes Advisor, 2023 г.

Импортонезависимый продукт. Российский разработчик

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

4 уровень доверия

АРПП Отечественный софт

Минцифры России

Sk Участник

РУС СОФТ

Клиенты

20+ клиентов из Топ 100 РБК

staffcop®

Актуально

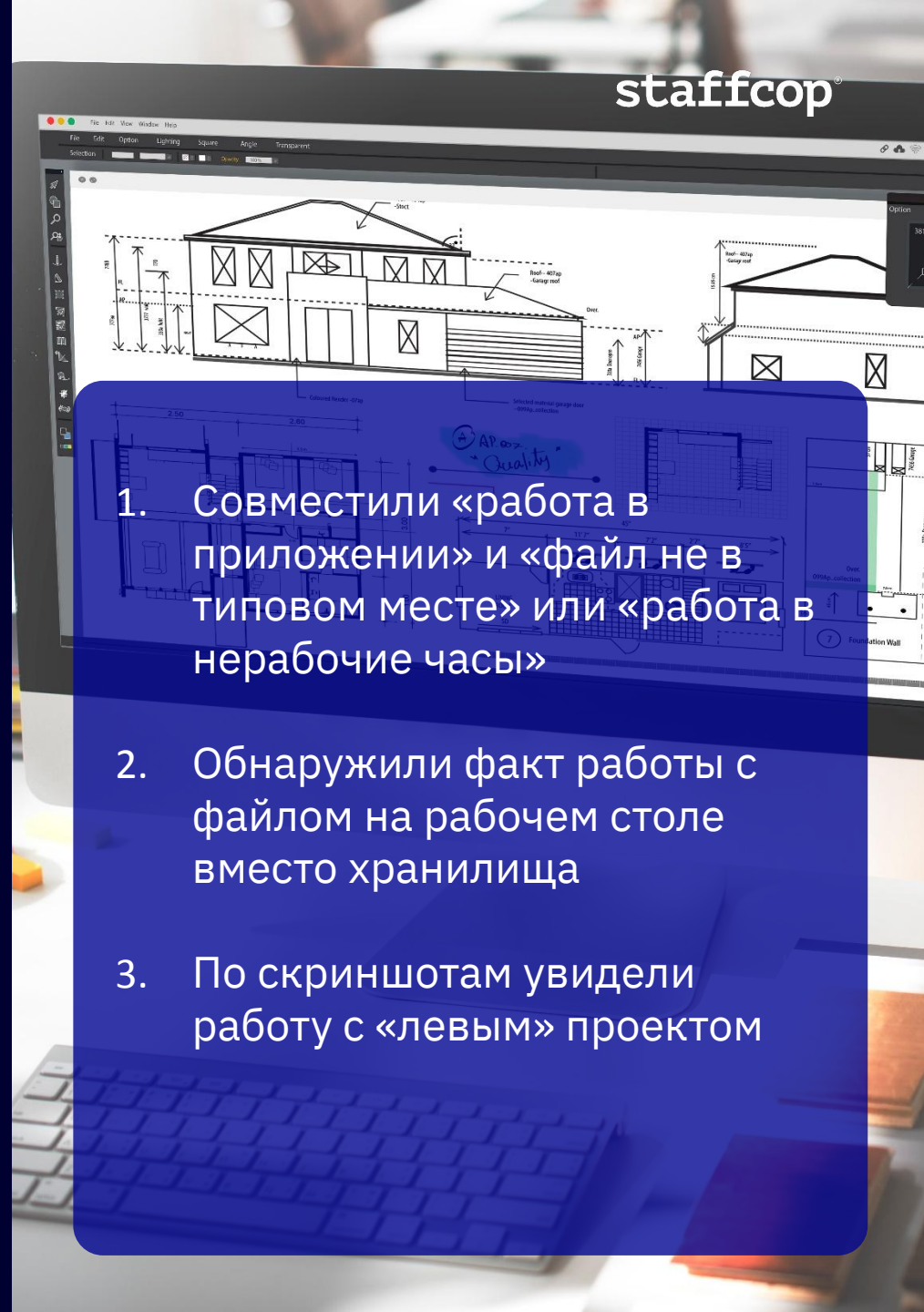
>66%

ИНСАЙДЕРЫ – ДОСТУПНЕЙ НЕ ПРИДУМАЕШЬ...

staffcop®

Кейс: проекты на стороне

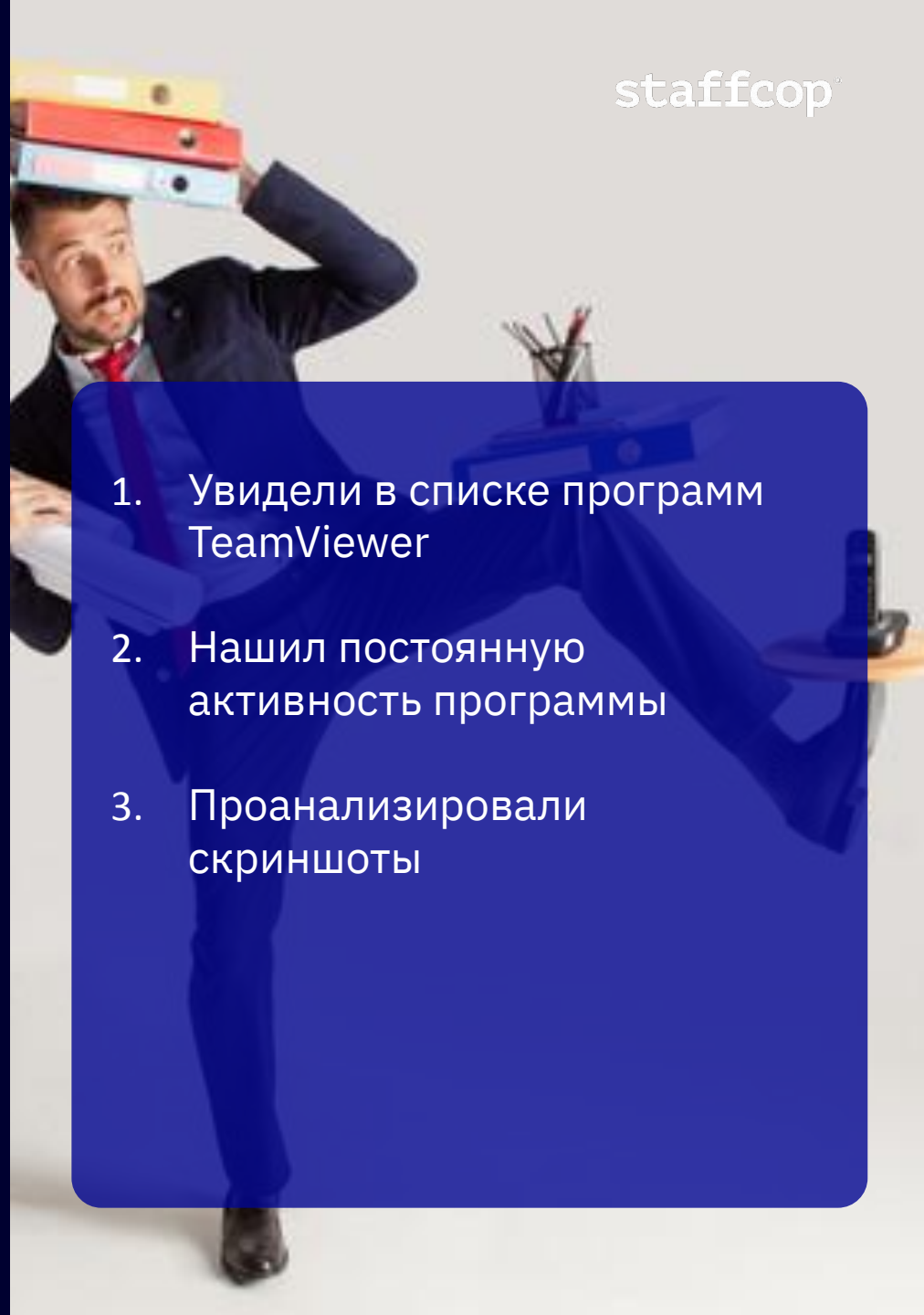
1. Кто: инженер конструкторского бюро работает более 10 лет!
2. Сотрудник работал над «левым» проектом от заказчика
3. Сотрудник работал над «левым» проектом на рабочем месте



1. Совместили «работа в приложении» и «файл не в типовом месте» или «работа в нерабочие часы»
2. Обнаружили факт работы с файлом на рабочем столе вместо хранилища
3. По скриншотам увидели работу с «левым» проектом

Кейс: параллельная работа

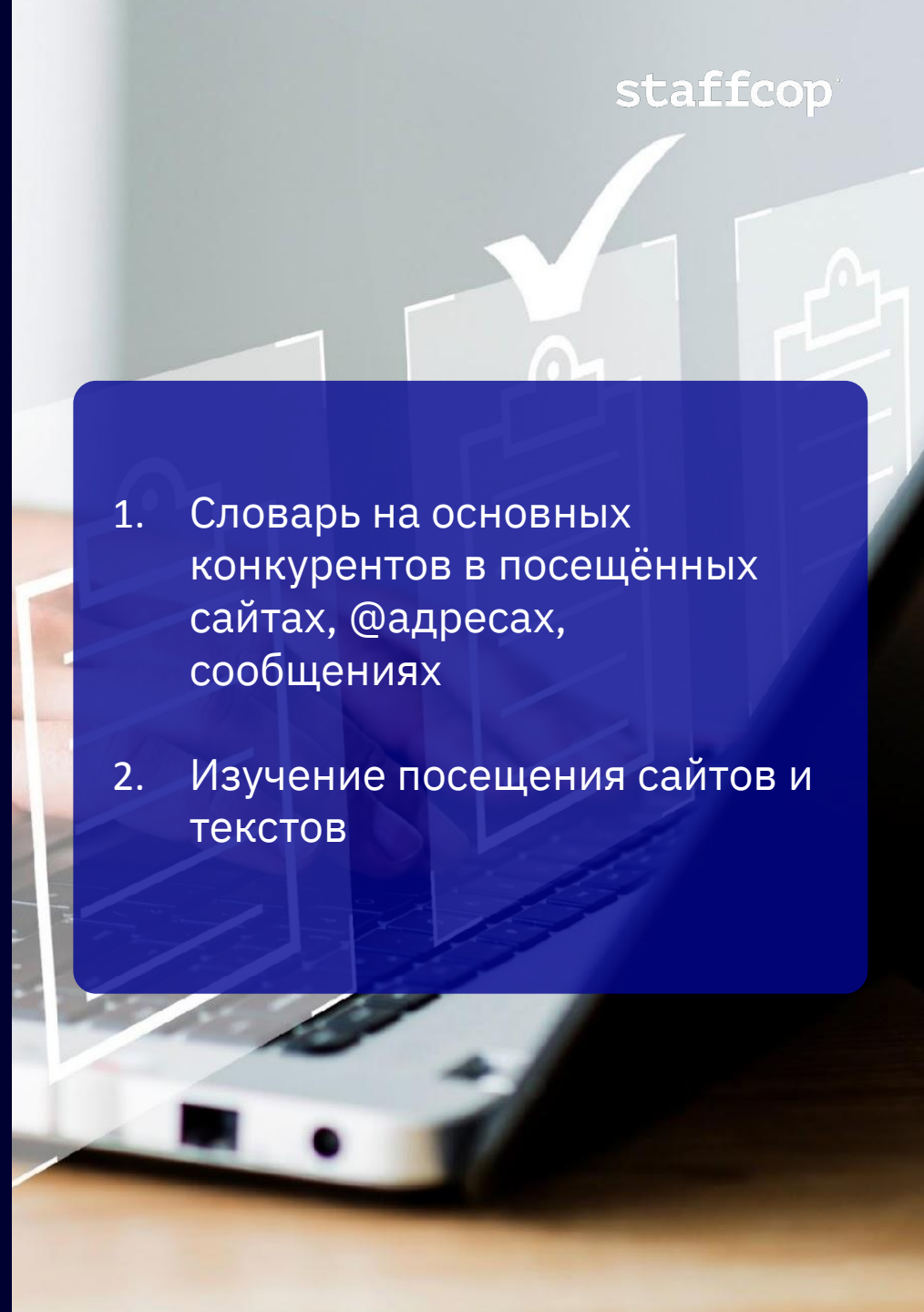
1. Кто: опытный бухгалтер
2. Подключалась к удаленному компьютеру с рабочего места
3. Параллельно с работой вела бухгалтерию в другом предприятии (в рабочее время с рабочего места)



1. Увидели в списке программ TeamViewer
2. Нашил постоянную активность программы
3. Проанализировали скриншоты

Кейс: подготовка к увольнению

1. Кто: сотрудник перед увольнением
2. Прошел собеседование к конкуренту
3. На рынке несколько основных игроков
4. «Готовился» к увольнению



1. Словарь на основных конкурентов в посещённых сайтах, @адресах, сообщениях
2. Изучение посещения сайтов и текстов

staffcop

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

Insider Risk Management

staffcop®

ИМПОРТОНЕЗАВИСИМОСТЬ – ПОЧЕМУ ИМЕННО СЕЙЧАС ЭТО РЕАЛЬНО ВАЖНО?

staffcop®

staffcop

Использование отечественного и независимого ПО

Технологии сервера:

open source initiative

ASTRA LINUX®

ClickHouse

PostgreSQL

OS рабочих ПК и АРМ:

base alt

ROSA

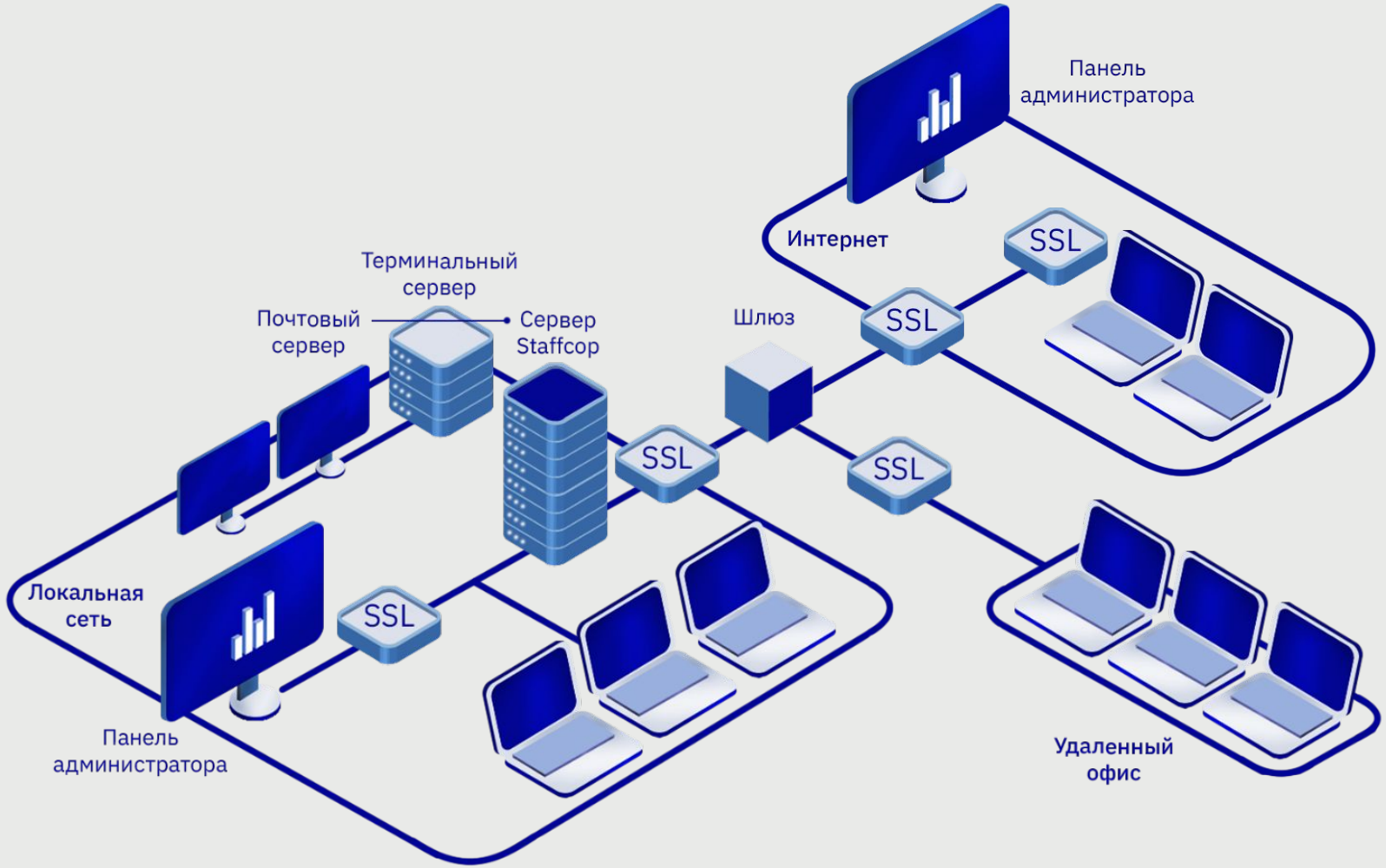
ASTRA LINUX®

РЕДОС

Компоненты, не требующие лицензирования и покупки

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



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®

Преимущества Staffcop Enterprise

Кроссплатформенный

Быстрый и легкий

Простое и доступное лицензирование

Импортонезависимый

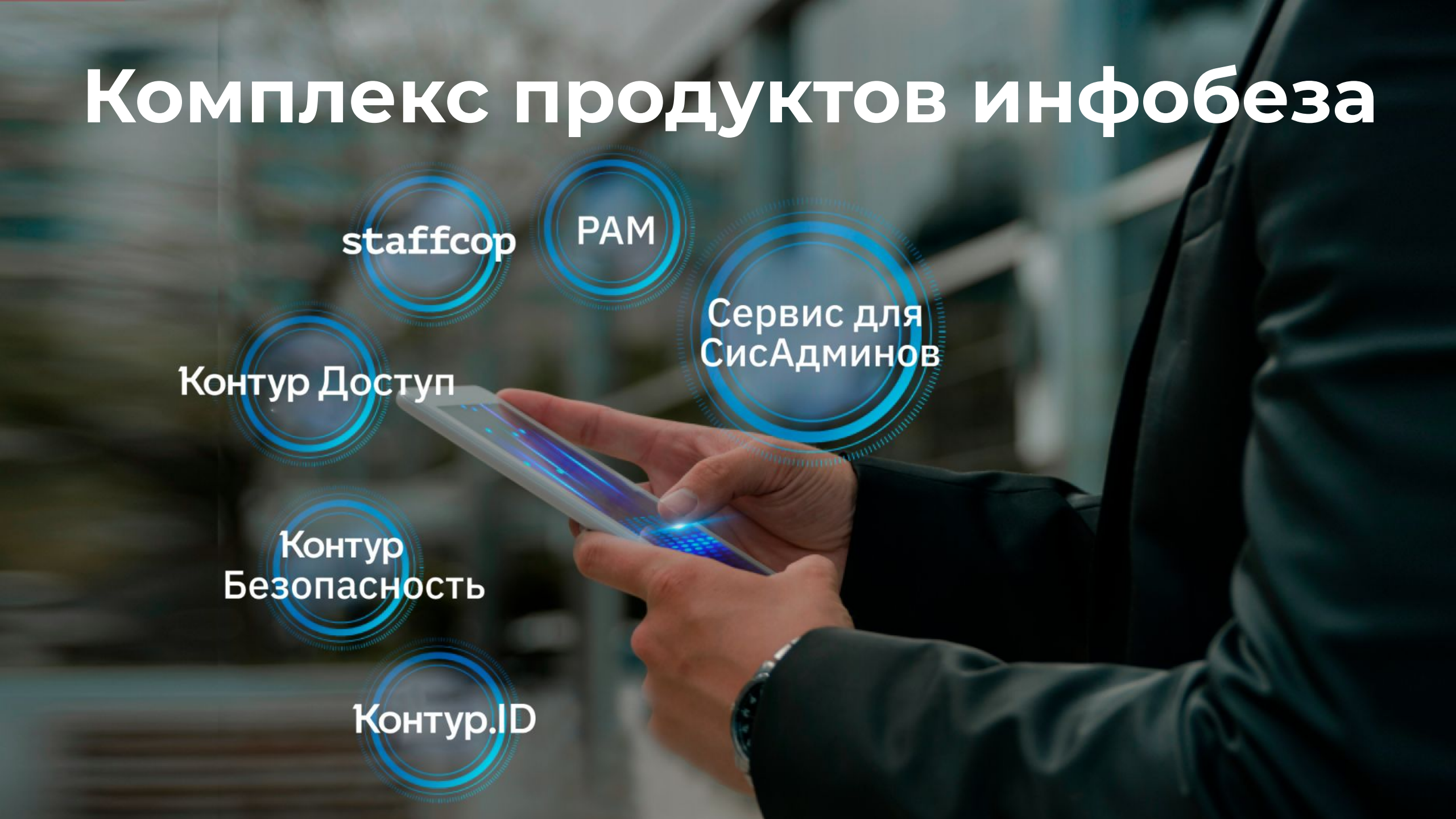
Качественная техническая поддержка

Индивидуальный подход, закрепленный менеджер

Расширенный пилот с полноценным функционалом

Доступ к регулярным обновлениям

Комплекс продуктов инфобеза



Staffcop Enterprise 5.5: эволюция внутренней безопасности

Ждем вас на вебинаре

30 октября в 11:00 по МСК

LIVE

Релиз 5.5 представят:

Даниил Бориславский,
заместитель генерального директора по развитию продукта

Александр Пицик,
технический директор

Станислав Юдинских,
руководитель проектов

Регистрация на вебинар

Узнайте больше о новых функциях и задайте вопросы в прямом эфире!

Ключевые фичи релиза 5.5

Анализ рисков:

Категоризация событий в реальном времени для приоритетного реагирования на угрозы.

Новый релиз Staffcop Enterprise 5.5 предлагает расширенные возможности анализа рисков и улучшенный мониторинг событий для повышения внутренней безопасности.

Учет активности в ВКС:

Контроль вовлеченности сотрудников и эффективности встреч.

Централизованная установка меток:

Маркировка файлов с чувствительной информацией для защиты от утечек.

Перехват командной строки:

Контроль привилегированных пользователей, перехват подозрительных команд в cmd и powershell.

Перехват RDP:

Мониторинг удаленных подключений и перехват файлов через буфер обмена.

Спасибо за внимание!

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

/ Уинстон Черчилль /

Юрий Драченин

Заместитель генерального директора
ООО «Атом Безопасность»
duu@staffcop.ru

staffcop.ru

Telegram

staffcop® Расследование инцидентов внутренней безопасности