УПРАВЛЕНИЕ ДОСТУПОМ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ К ИТ-СИСТЕМАМ ОРГАНИЗАЦИИ

Сценарии и практика применения

INDEED ID

О НАШЕЙ КОМПАНИИ

Компания Индид — российский вендор программного обеспечения для повышения информационной безопасности в компаниях разных отраслей экономики.

5
ОФИСОВ В МИРЕ
Москва, Санкт-Петербург, Великий Новгород, Вильнюс, Сингапур

3
ПРОДУКТА
в Реестре отечественного ПО

3
РЕГИОНА ПРИСУТСТВИЯ
СНГ, Европа, Юго-Восточная Азия

200+
ВЫПОЛНЕННЫХ ПРОЕКТОВ

10
ЛЕТ ОПЫТА
Проектирование, разработка, тестирование и внедрение комплексных решений

50+
СОТРУДНИКОВ
Распределенная команда: 4 региона, 3 страны

4
ПРОДУКТА
Полностью самостоятельная разработка

INDEED ID

ИТОГИ 2020*
ВОЗМОЖНО ЛИ РАЗВИТИЕ ВО ВРЕМЯ ПАНДЕМИИ?

+60 000

Новых пользователей защищены решениями Индид

210%

Рост количества завершенных проектов

30%

Рост числа сотрудников

18%

Рост оборота в Европе и Азии

+8

Релизов по трем продуктам

50%

Рост оборота в России и СНГ

*по сравнению с 2019 годом

НАШИ ПРОДУКТЫ

Все продукты находятся в Реестре отечественного программного обеспечения

INDEED ACCESS MANAGER

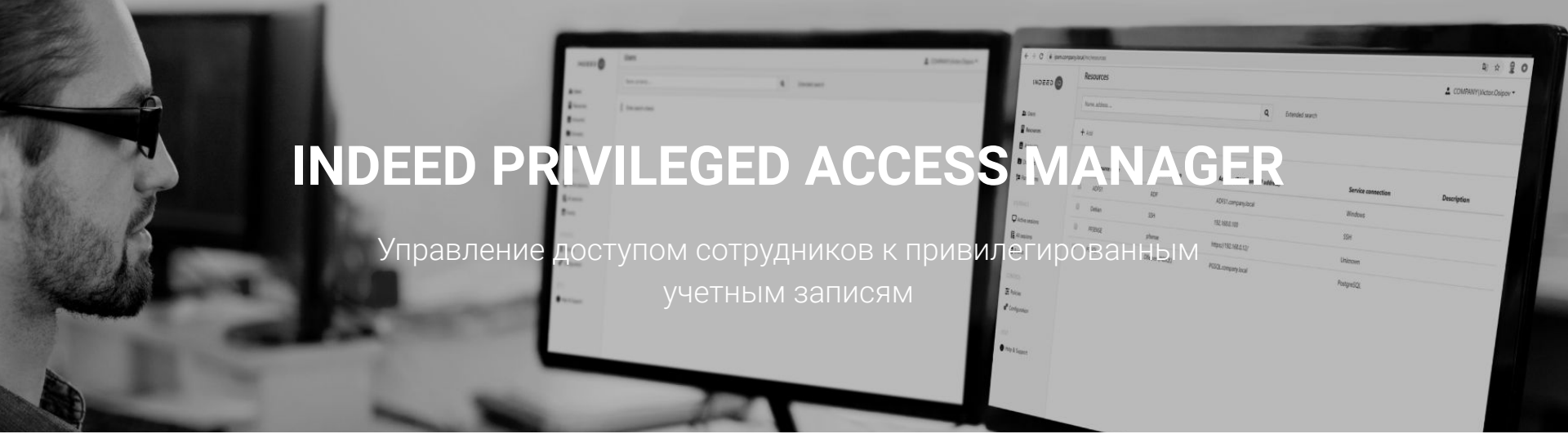
Управление доступом пользователей к IT-ресурсам компании

INDEED PRIVILEGED ACCESS MANAGER

Управление и защита доступа к привилегированным учетным записям

INDEED CERTIFICATE MANAGER

Централизованное управление инфраструктурой открытых ключей и носителями цифровых сертификатов



INDEED PRIVILEGED ACCESS MANAGER

Управление доступом сотрудников к привилегированным учетным записям

Сохранение в секрете паролей учетных записей

Видео и текстовая запись сессий

Обнаружение привилегированных учетных записей

Двухфакторная аутентификация

INDEED ID

АКТУАЛЬНОСТЬ

30%

Средний ежегодный рост количества удаленных сотрудников в год, 2020

Исследование удаленной работы в мире статистика от FYI 2020

59%

Учетных записей относятся к внешним сотрудникам, подрядчикам, поставщикам. Balabit, 2018, весь мир

IT out of control

70%

Компаний утверждают, что у них увеличилось количество привилегированных пользователей. Balabit, 2018, весь мир

IT out of control

44%

Всех утечек данных в 2017 г. были связаны с привилегированными учетными записями. Balabit, 2018, весь мир

44% of data breaches in the last year involved privileged identity according to global Balabit research report

ИНЦИДЕНТ В SIEMENS

23.07.2019

Подрядчик закладывал «логические бомбы» в поддерживаемые им электронные таблицы

Через некоторый период таблицы начали сбоить, и его снова нанимали. Не был обнаружен с 2014 по 2016 годы. Работал с Siemens на протяжении 8 лет. Наказание: штраф 250 000$ или лишение свободы до 10 лет

INDEED ID

ИНЦИДЕНТ В SHIONOGI

23.07.2019

Админа поймали на саботаже бывшего работодателя

Дочка японской фармкомпании в США. ИТ-сотрудник оставил “backdoor”(закладку) для удаленного доступа к критичным компонентам. Удаленно нарушил работу 88 серверов: почта, сервер BlackBerry, сервер обработки заказов и др. Потери: прямые — 800 000$; паралич деятельности компании на 5 дней

ПРОБЛЕМЫ ДОСТУПА ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Угроза безопасности: сбой критичных компонентов, кража паролей

Слабо защищенный удаленный доступ администраторов и подрядчиков к критичным компонентам ИТ-инфраструктуры — источник повышенной опасности.

Сложность контроля работы с компонентами, критичными для бизнеса

Контроль действий привилегированных пользователей осуществляется через DLP-системы,, которые неприменимы на сетевых устройствах, серверах Linux, или на рабочих станциях подрядчиков.

Финансовые и временные потери

Вынужденная локальная работа подрядчиков и администраторов с критичными компонентами снижает оперативность реагирования на сбои. В любом формате доступа затруднен учет реального объема работ.

Простой работы ресурсов и снижение производительности труда администраторов ИБ

Дополнительные трудо- и времязатраты на расследование сбоя или инцидента при использовании данных из SIEM, т.к. они не показывают полную картину причин инцидента и виновных.

ПЛАТФОРМА INDEED PAM

Управляет доступом привилегированных пользователей и фиксирует их действия

Экономия времени и финансов предприятия

Защищенный и контролируемый удаленный доступ подрядчиков и администраторов к критичным компонентам ИТ-инфраструктуры. Инструменты оценки объема работ подрядчиков и администраторов систем управления технологическими процессами.

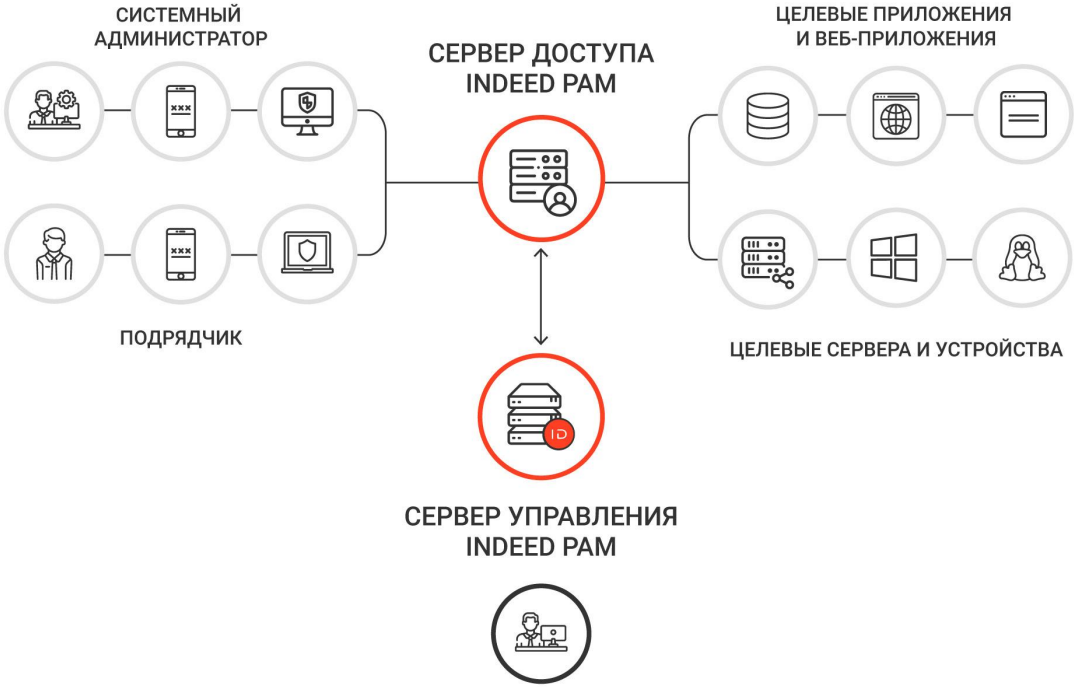
Минимизация угроз сбоя критичных компонентов и кражи пароля

Единая система управления доступом к привилегированным учетным записям и целевым ресурсам с защитой от несанкционированного обхода. Содержит механизм двухфакторной аутентификации для беспрепятственного предоставления удаленного доступа только доверенному пользователю.

Снижение времени простоя ресурсов и повышение производительности труда администраторов ИБ

Различные механизмы контроля и фиксации действий сотрудников с последующим анализом записей действий сотрудников для оперативной локализации инцидентов.

ОПИСАНИЕ ТЕХНОЛОГИИ



Поддержка протоколов:

- RDP
- SSH
- HTTP(S)
- Иные проприетарные протоколы через публикацию приложений

Поддержка управления паролями целевых ресурсов:

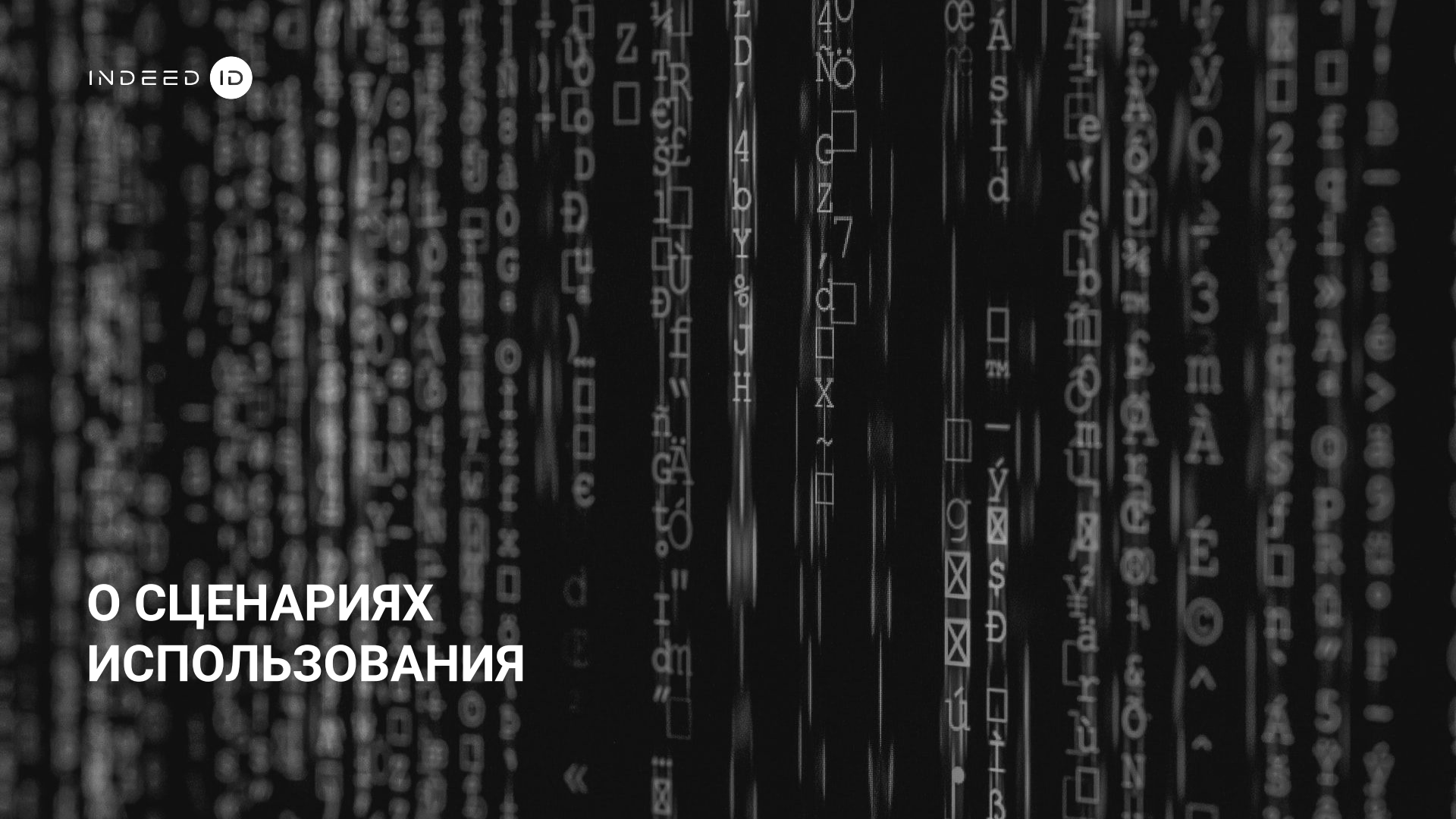
- MS Active Directory
- MS Windows
- Linux/Unix
- СУБД (PostgreSQL, MS SQL, MySQL, Oracle DB)
- Web-Application
- Desktop Application

Поддержка способов контроля действий:

- Видеозапись
- Текстовая запись
- Снимки экрана
- Теневое копирование файлов
- Блокировка ввода команд
- Разрыв удалённого подключения

Поддержка интеграции:

- SIEM (syslog)
- Mail (SMTP)
- IdM
- API



О СЦЕНАРИЯХ ИСПОЛЬЗОВАНИЯ

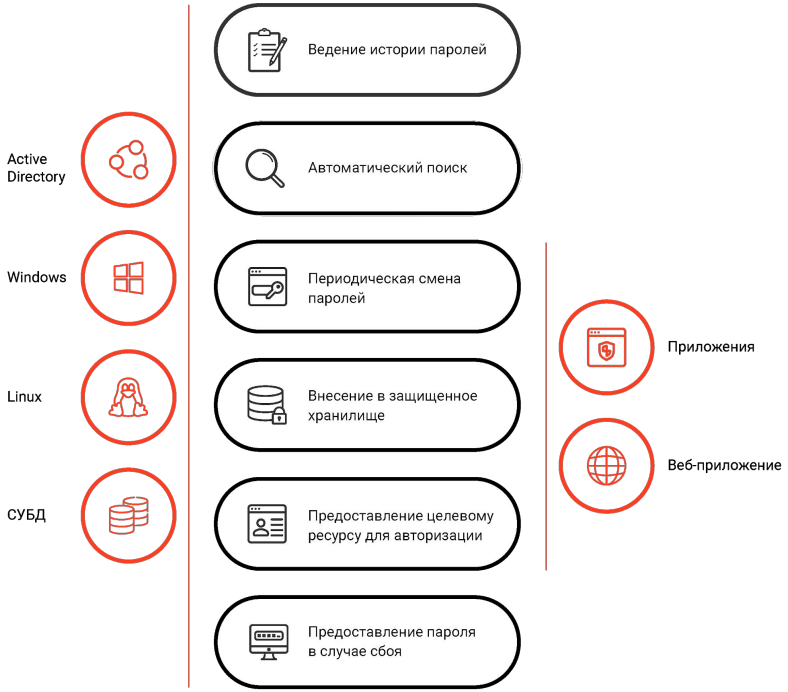
ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

INDEED ID

УПРАВЛЕНИЕ ПАРОЛЯМИ УЧЕТНЫХ ЗАПИСЕЙ

Основные возможности:

- Защищенное хранилище привилегированных учетных записей
- Автоматический поиск и импорт учетных записей
- Управление паролями
- Коннекторы к целевым ресурсам для сквозной аутентификации



INDEED ID

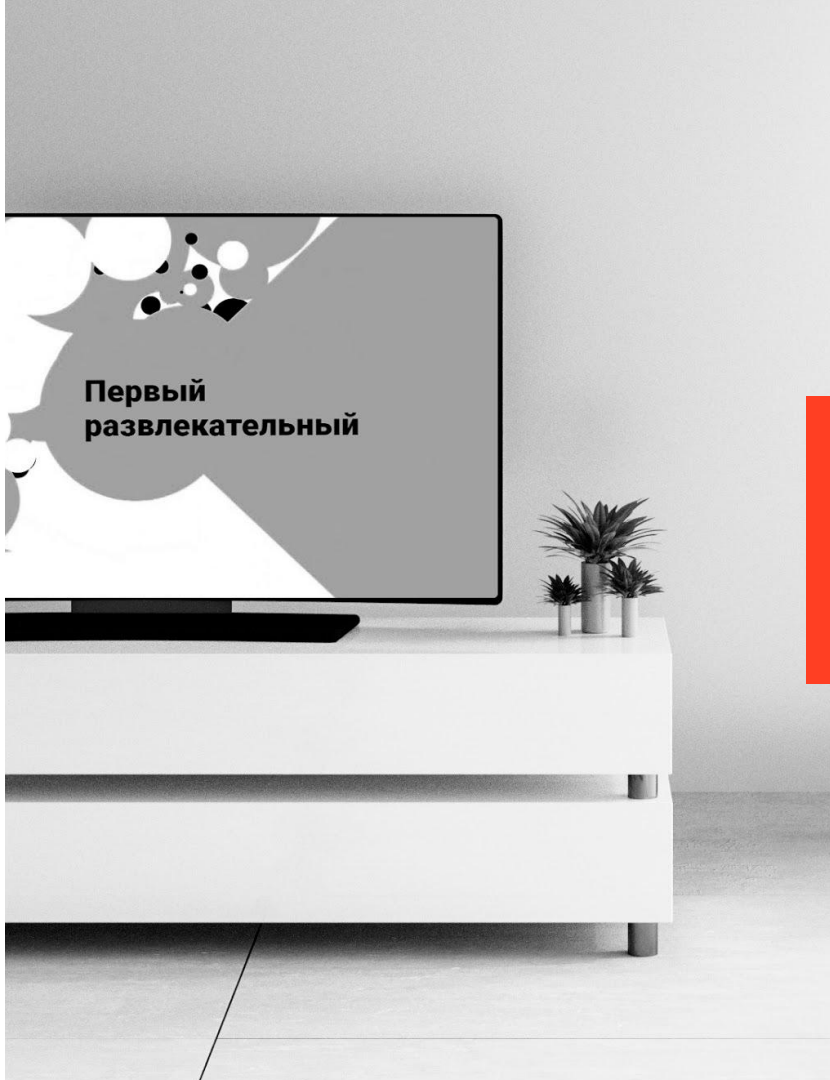
ЕДИНАЯ ТОЧКА УДАЛЕННОГО ДОСТУПА

- Единый инструмент управления привилегированным доступом
- Минимизация полномочий привилегированных пользователей
- Двухфакторная аутентификация
- Интеграция с Active Directory
- Поддержка протоколов: RDP, SSH, HTTP(S)
- Поддержка публикации приложений

КЕЙС — СТС МЕДИА

- Обеспечена единая точка входа для привилегированных пользователей разных доменов с ресурсами опубликованными через терминальные серверы на разных площадках
- Используются механизмы многофакторной аутентификации привилегированных пользователей
- Реализован контроль доступа к опубликованным на терминальных серверах корпоративным приложениям

Масштаб: более 100 пользователей

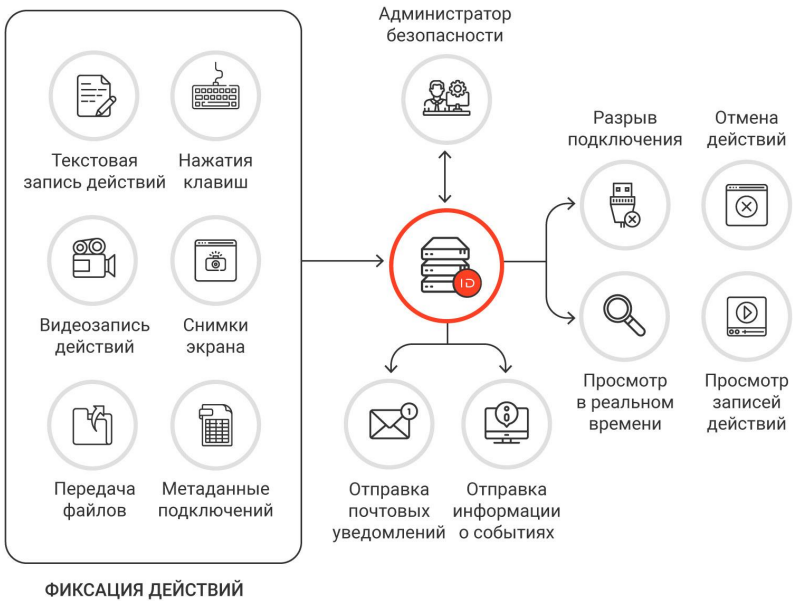


INDEED ID

ЗАПИСЬ ДЕЙСТВИЙ ДЛЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

Повышение эффективности реагирования:

- Разные способы фиксации действий
- Блокировка операций и разрыв соединения
- Мониторинг в режиме реального времени
- Просмотр записей событий
- Избежание необоснованных обвинений сотрудников



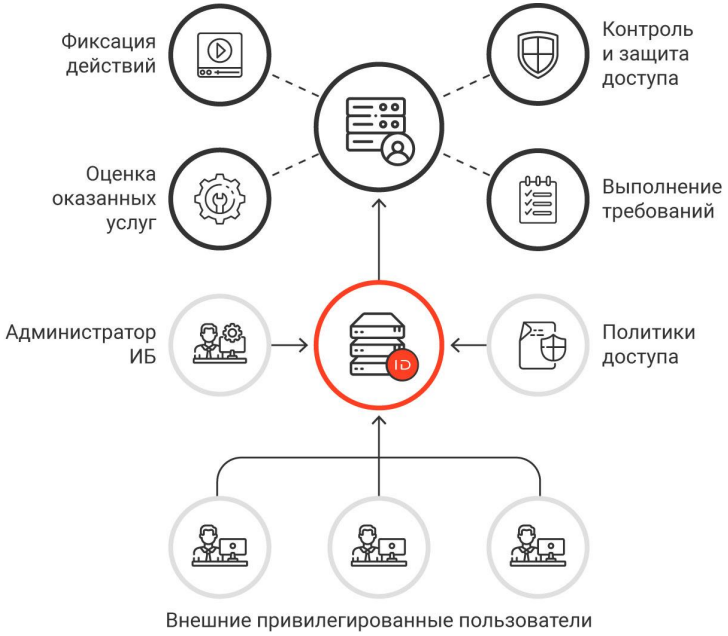
КЕЙС — ФЕДЕРАЛЬНОЕ МИНИСТЕРСТВО

- Большое количество целевых ресурсов и привилегированных пользователей разных категорий
- Для подключений разной критичности настроены индивидуальные параметры записи действий
- Заказные доработки для повышения эффективности контроля действий и реагирования на инциденты

Масштаб: 200 пользователей

КОНТРОЛИРУЕМЫЙ ДОСТУП ПОДРЯДЧИКОВ

- Контролируемый и защищенный удаленный доступ
- Запись всех действий
- Оценка качества работы
- Экономия времени и ресурсов
- Ограничение доступа по расписанию и по согласованию
- Контроль работы инженеров и специалистов технической поддержки
- Контроль работы аудиторов и разработчиков



КЕЙС — О`КЕЙ ГРУПП

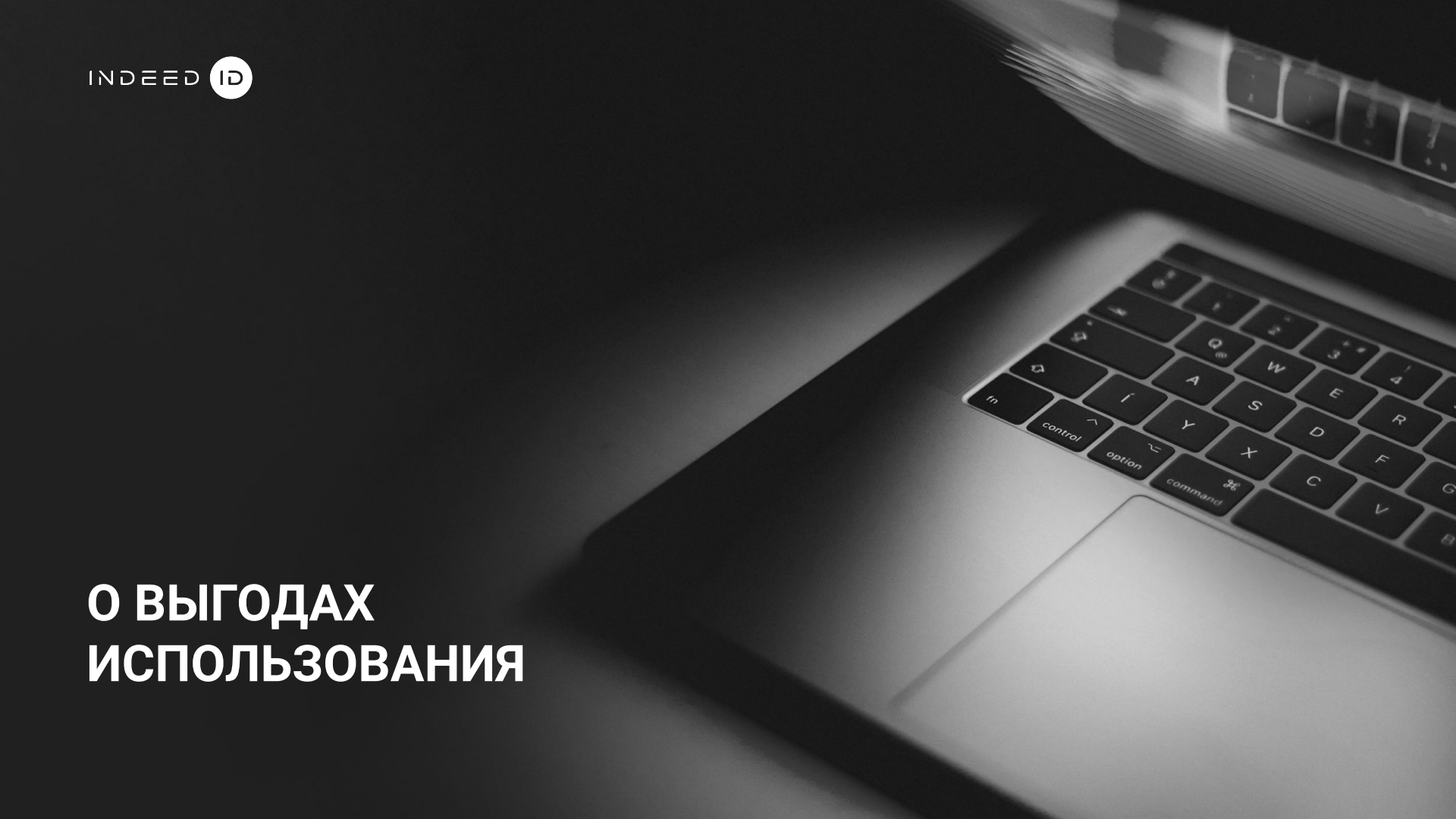
- Внедрена система защиты и управления доступом к привилегированным учетным записям
- Обеспечено исключение знания секрета (пароли) привилегированными пользователями при подключении к целевым ресурсам
- Для реализации задач контроля используется механизм, позволяющий персонифицировать подключения
- Реализован процесс контроля действий и оценки заявленного качества услуг внешних привилегированных пользователей

Масштаб: более 100 пользователей

INDEED PAM КАК СЕРВИС

- Установка одного или нескольких серверов доступа PAM на мощностях ЦОД или SOC
- Экономия бюджетных средств и трудозатрат за счет централизованного развертывания
- Единые подходы к организации контроля удаленных подключений
- «Замыкание» административного доступа на сервера PAM
- Единая точка входа для всех удаленных подключений
- Заключение соглашений с клиентами и партнерами об осуществлении контроля удаленных подключений
- Единый узел мониторинга и управления удаленными административными подключениями

INDEED



О ВЫГОДАХ ИСПОЛЬЗОВАНИЯ

ПРЕИМУЩЕСТВА INDEED PAM

Расширенная функциональность управления паролями и привилегированными учётными записями, включая их автоматический поиск, защищенное хранение и обновление.

Доступ ко всем функциональным возможностям программного комплекса без приобретения дополнительных лицензий.

Интеграция с любыми целевыми системами, включая системы безопасности (СКУД, IdM, SIEM)

ПОСТРОЕНИЕ БИЗНЕС-ПРОЦЕССА

Организационно-распорядительная документация		Техническая документация	
Зачем это нужно?	Положения и регламенты на процесс контроля	Правильно ли это внедрено?	Документы на внедрение
Как часто это используется?	Распределение нагрузки (подключений) на систему	Как это работает?	Сетевые схемы работы (встраивания)
Кто с этим работает?	Программа и план обучения сотрудников	Как этим пользоваться?	Технические инструкции
Насколько это полезно?	Методика периодической оценки эффективности	Чем это управляет?	Матрица доступа и полномочий

*Для разработки документации рекомендуем обратиться к нашим партнерам

INDEED ID

КЕЙС — БАНК «САНКТ-ПЕТЕРБУРГ»

- Долгая история партнерства и высокая оценка качества совместной работы
- Реализована “экосистема” управления доступом от компании Индид
- Проведена замена конкурирующего иностранного решения
- Уменьшена общая стоимость владения системой контроля действий привилегированных пользователей

Масштаб: 200 пользователей

INDEED ID

КЕЙС — ГРУППА КОМПАНИЙ «ЕПК»

- Защита доступа и контроль действий привилегированных пользователей при управлении технологическими процессами на промышленном предприятии
- Реализованы инструменты удаленного контроля за действиями привилегированных пользователей со стороны сотрудников информационной безопасности

Масштаб: 50 пользователей

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Программные комплексы компании Индид помогают соответствовать требованиям нормативно-правовых актов и стандартов

ISO 27001.2013
(менеджмент информационной безопасности)

PCI DSS V.3.2.1 от 05.2018
(защита данных держателей карт)

Приказ ФСТЭК № 17 от 11.02.2013
(защита ГИС)

Приказ ФСТЭК № 21 от 18.02.2013
(защита ПДн)

Приказ ФСТЭК № 31 от 14.03.2014
(защита АСУ ТП)

Приказ ФСТЭК № 239 от 25.12.2017
(защита ОКИИ)

ГОСТ 57580.1-2017
(защита финансовых операций)

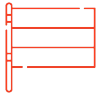
Приказ ФАПСИ №152
(порядок использования СКЗИ)

INDEED

ПРЕИМУЩЕСТВА КОМПАНИИ

Поддержка 24/7 с возможностью выезда инженера

Доработка решений под задачи заказчика



Российский разработчик программного обеспечения

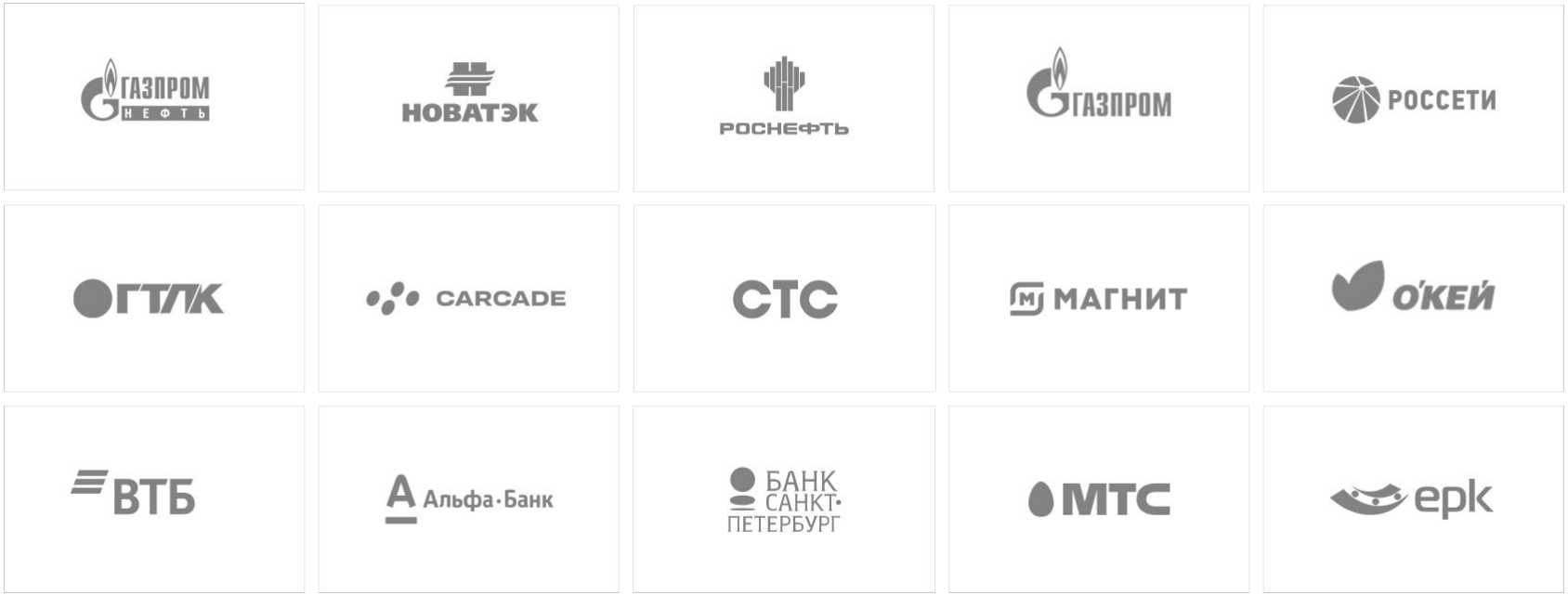
Бесплатное тестирование продуктов с предоставлением оборудования

Организация референсов и презентаций

Партнерская программа

INDEED ID

НАШИ ЗАКАЗЧИКИ



INDEED ID

КОНТАКТЫ

indeed-id.ru

inbox@indeed-id.com

8 (800) 333-09-06