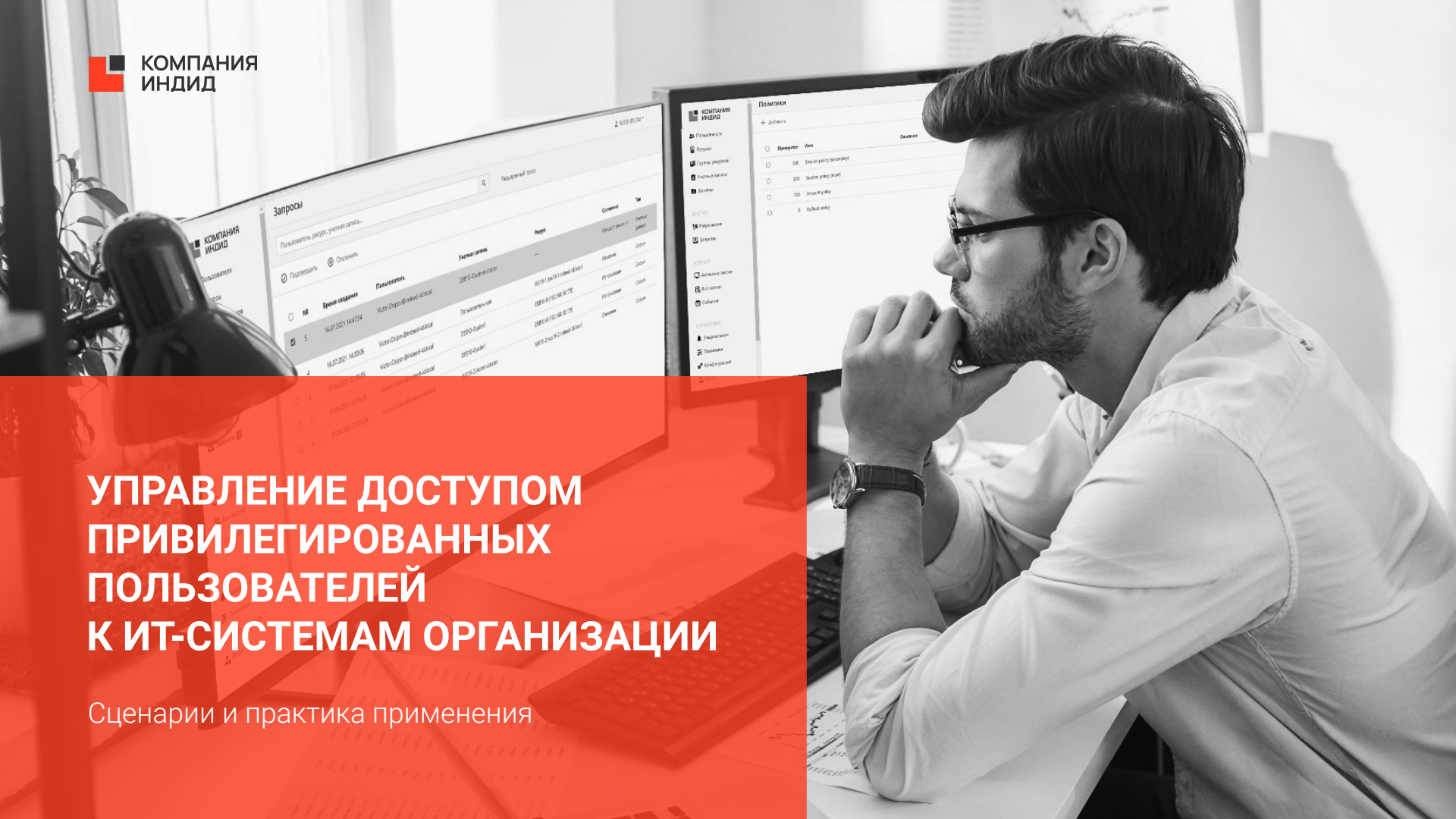
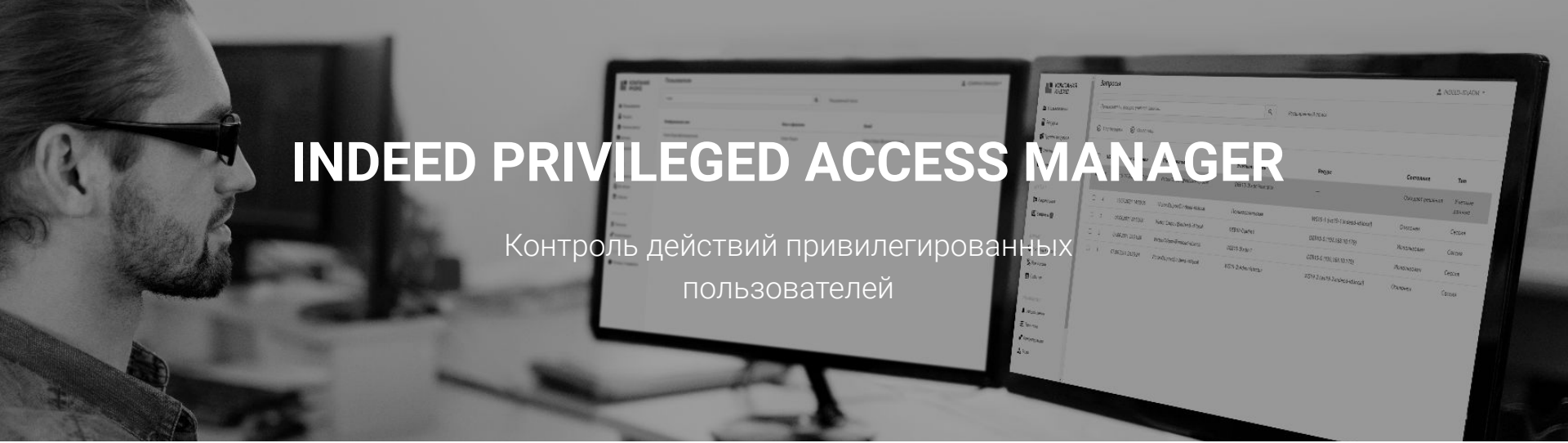
КОМПАНИЯ ИНДИД



УПРАВЛЕНИЕ ДОСТУПОМ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ К ИТ-СИСТЕМАМ ОРГАНИЗАЦИИ

Сценарии и практика применения



INDEED PRIVILEGED ACCESS MANAGER

Контроль действий привилегированных пользователей

Контроль административных учетных записей

Разные способы записи и анализа действий

Управление привилегированным доступом

Двухфакторная аутентификация

ПРОБЛЕМЫ КОНТРОЛЯ АДМИНИСТРАТОРОВ

ОТСУТСТВИЕ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ

Кража данных, нарушение работы критичных компонентов

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

Слабый контроль работы администраторов или подрядчиков

Контроль действий привилегированных пользователей не осуществляется, либо осуществляется частично через не предназначенные для этого инструменты.

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Лишние расходы на организацию работы

Затруднен учет реального объема работ и соблюдения требований SLA. Локальная работа с критичными компонентами требует затрат на логистику и снижает оперативность реагирования на сбои.

Снижение производительности труда офицеров безопасности

Чрезмерные трудозатраты на расследование сбоя или инцидента при использовании данных из “классических” систем мониторинга, т.к. они не показывают полную картину причин инцидента и виновных.

НЕЭФФЕКТИВНЫЕ ЗАТРАТЫ РЕСУРСОВ

ПРОБЛЕМАТИКА
И ИНЦИДЕНТЫ

100%

Компаний используют словарные пароли, в т.ч. для административных учетных записей, Positive Technologies

Подробнее

70%

Компаний утверждают, что у них увеличилось количество прив.пользователей, Balabit / OneIdentity

Подробнее

59%

Учетных записей в компании, в среднем, относятся к внешним сотрудникам, подрядчикам. Balabit / OneIdentity

Подробнее

23.07.2019

Подрядчик закладывал «логические бомбы» в поддерживаемые им электронные таблицы

Подробнее

Весна-лето 2022 г.

Злоумышленники украли и выложили в открытый доступ базы данных пользователей известных российских компаний

РАСПРЕДЕЛЕННОЕ
УПРАВЛЕНИЕ ДОСТУПОМ

Поддержка протоколов:

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

Поддержка управления паролями целевых ресурсов:

- Active Directory / OpenLDAP* / FreeIPA*
- 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 удаленного подключения

Поддержка интеграции:

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

* Поддержка OpenLDAP / FreeIPA - в I-II кв. 2023 г.

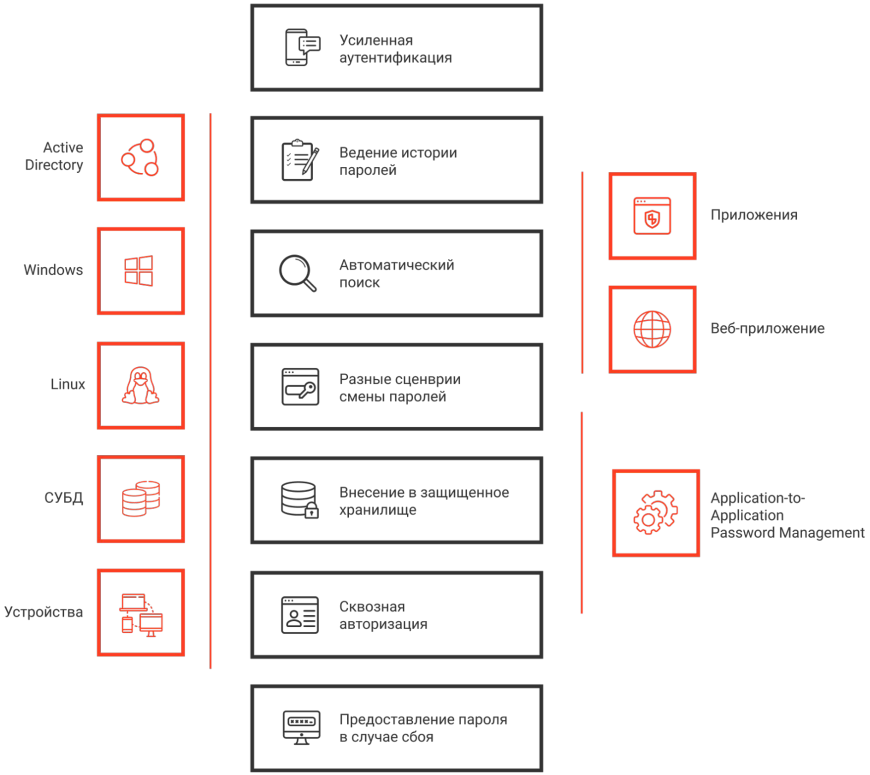
КОМПАНИЯ
ИНДИД

КАТЕГОРИЗАЦИЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

УПРАВЛЕНИЕ ПАРОЛЯМИ УЧЕТНЫХ ЗАПИСЕЙ

Основные возможности:

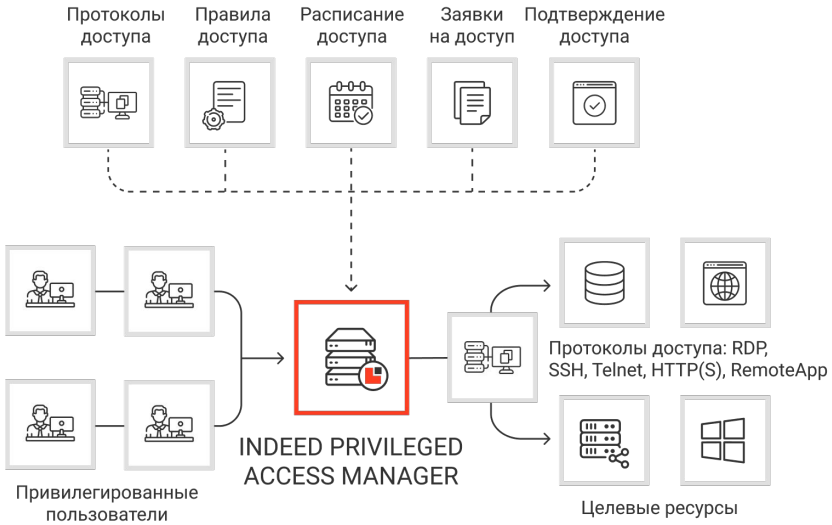
- Автоматический поиск и импорт учетных записей
- Управление паролями (обновление, выдача, сброс после подключения)
- Поддержка пользовательских учетных записей
- Enterprise Single Sign-On для целевых приложений
- Усиленная аутентификация
- Application-to-Application Password Management



ЕДИНАЯ ТОЧКА
УДАЛЕННОГО ДОСТУПА

- Единый инструмент управления привилегированным доступом
- Интеграция с ServiceDesk
- Интеграция с Active Directory, OpenLDAP*, FreeIPA*
- Импорт ресурсов из Active Directory, OpenLDAP*, FreeIPA* и CSV
- Поддержка протоколов: RDP, SSH, Telnet, HTTP(S)
- Поддержка публикации приложений (RemoteApp & Microsoft RDS)

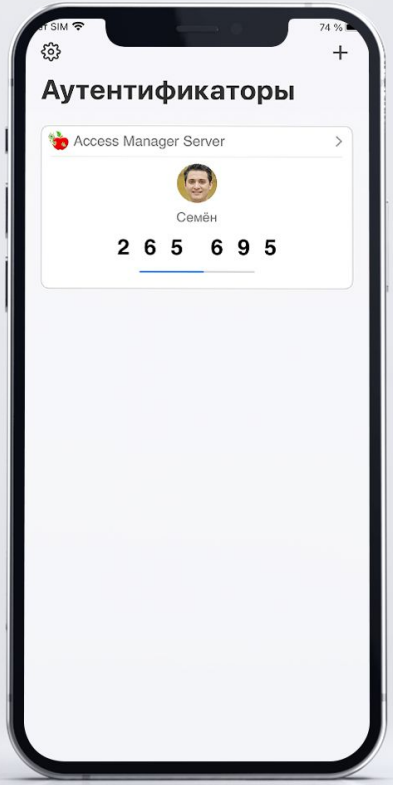
* Поддержка OpenLDAP и FreeIPA - в версии 2.8 в I-II кв. 2023 г.



КОМПАНИЯ
ИНДИД

INDEED KEY: МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ДЛЯ ЗАЩИТЫ ДОСТУПА

- Поддержка протокола аутентификации TOTP (одноразовые пароли)
- Поддержка аутентификации через push-уведомления*
- Удобство применения для локального и удаленного доступа



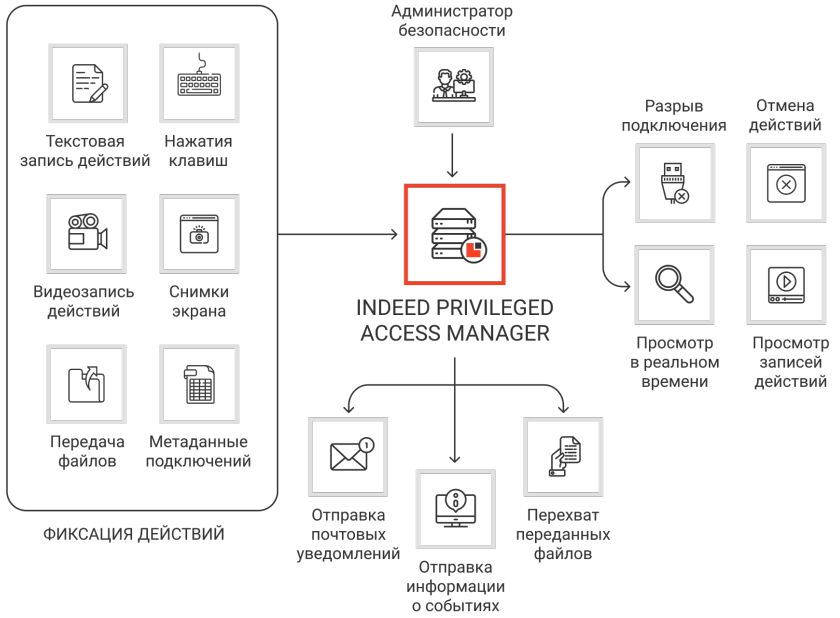
* Поддержка аутентификации через push-уведомления будет осуществляться через интеграцию с Indeed Access Manager и появится в IV кв. 2022 г.

ФИКСАЦИЯ И КОНТРОЛЬ ДЕЙСТВИЙ

Повышение эффективности реагирования:

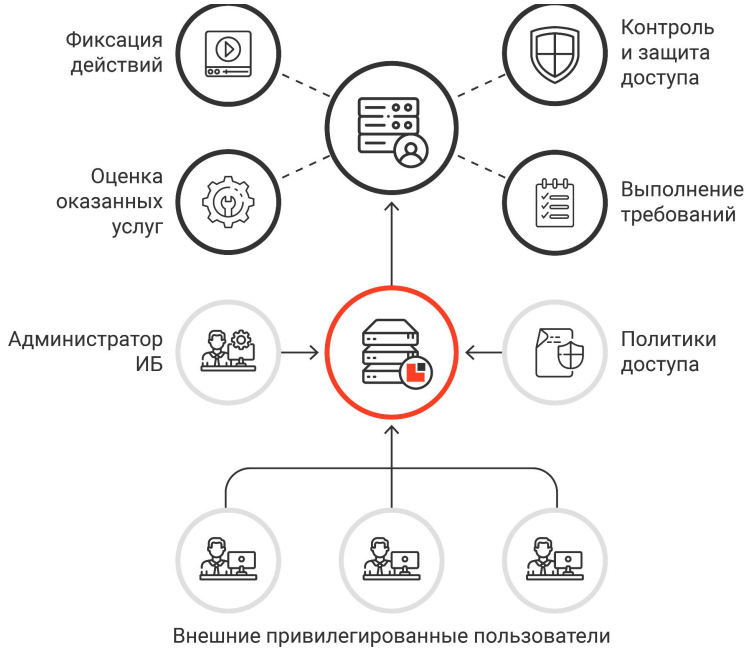
- Разные способы записи активности привилегированных пользователей
- Фильтрация текстовых команд и разрыв соединения (SSH)
- Мониторинг в режиме реального времени
- Просмотр записей событий и сквозной текстовый поиск
- Перехват и теневое копирование передаваемых файлов (RDP, SCP, SFTP*)

* SFTP - в версии 2.8 в I-II кв. 2023 г.



КОНТРОЛИРУЕМЫЙ ДОСТУП ПОДРЯДЧИКОВ

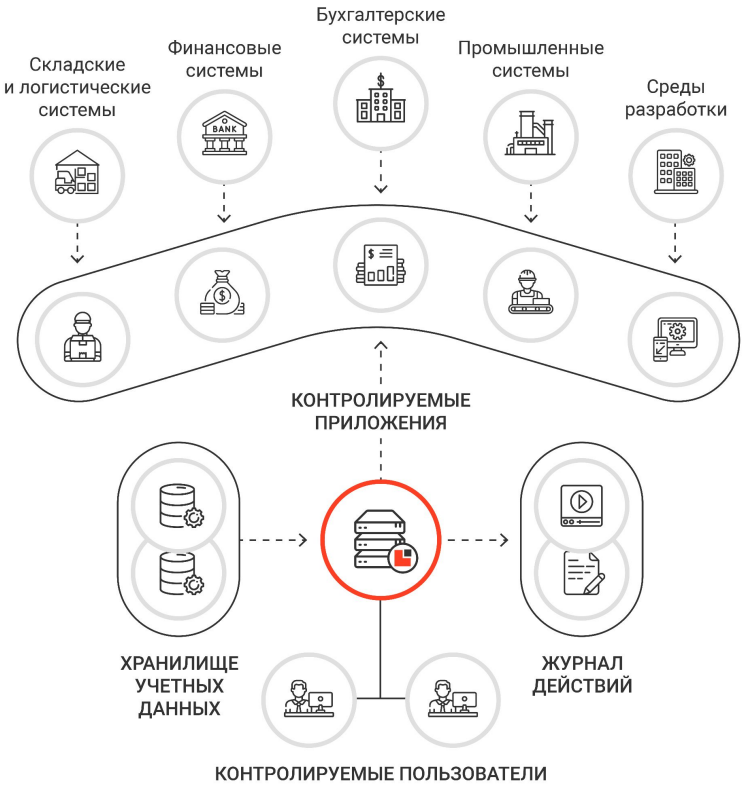
- Запись активности подрядчиков при работе с ИТ-ресурсами
- Данные для оценки качества работы
- Экономия времени и ресурсов при предоставлении доступа
- Ограничение доступа по расписанию и по согласованию
- Контроль работы инженеров и специалистов технической поддержки
- Контроль работы аудиторов и разработчиков



КОМПАНИЯ
ИНДИД

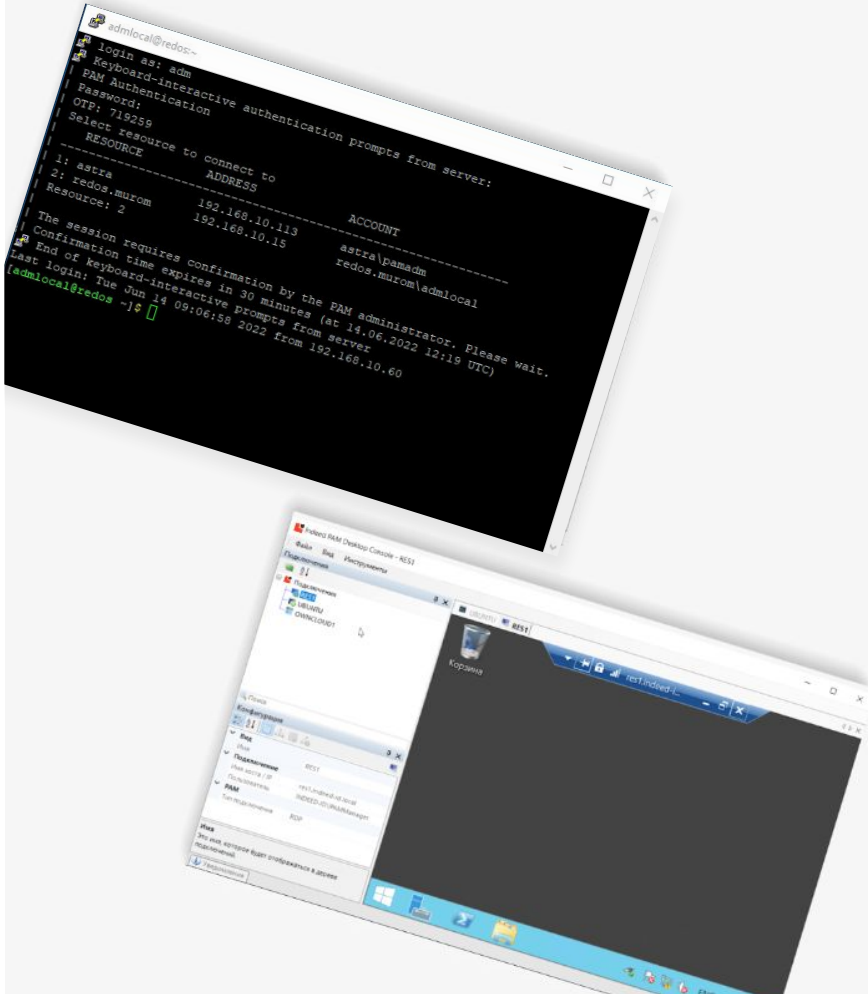
ЗАЩИЩЕННЫЙ ДОСТУП К КОРПОРАТИВНЫМ СЕРВИСАМ

- Публикация любых приложений
- Инструмент оперативной организации временного удаленного доступа к сервису
- Дополнительные функции защиты и контроля для сервера приложений
- Фиксация действий для анализа
- Сохранение паролей целевых приложений в секрете от сотрудника



ЧЕТЫРЕ СПОСОБА ПОДКЛЮЧЕНИЯ К РЕСУРСАМ

- Скачиваемый RDP-файл с уже готовыми настройками подключения к конкретному ресурсу (для подрядчиков)
- Строка подключения для клиентских приложений (для консольных подключений)
- Прямое подключение на соответствующий сетевой порт на IP-адресе шлюза доступа с использованием стандартного ПО (Putty)
- Программное обеспечение - менеджер удаленных подключений - содержит все доступные для пользователя подключения (для администраторов)



ПРИМЕНЕНИЕ INDEED PAM
В КОРПОРАТИВНОМ ЦОД

- Для размещения в ЦОД и предоставления услуг ИБ
- Поддержка отказоустойчивых конфигураций
- 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
- Единый узел мониторинга и управления удаленными административными подключениями

ВЫГОДЫ ОТ ПРИМЕНЕНИЯ INDEED PRIVILEGED ACCESS MANAGER

Экономия времени и финансов предприятия

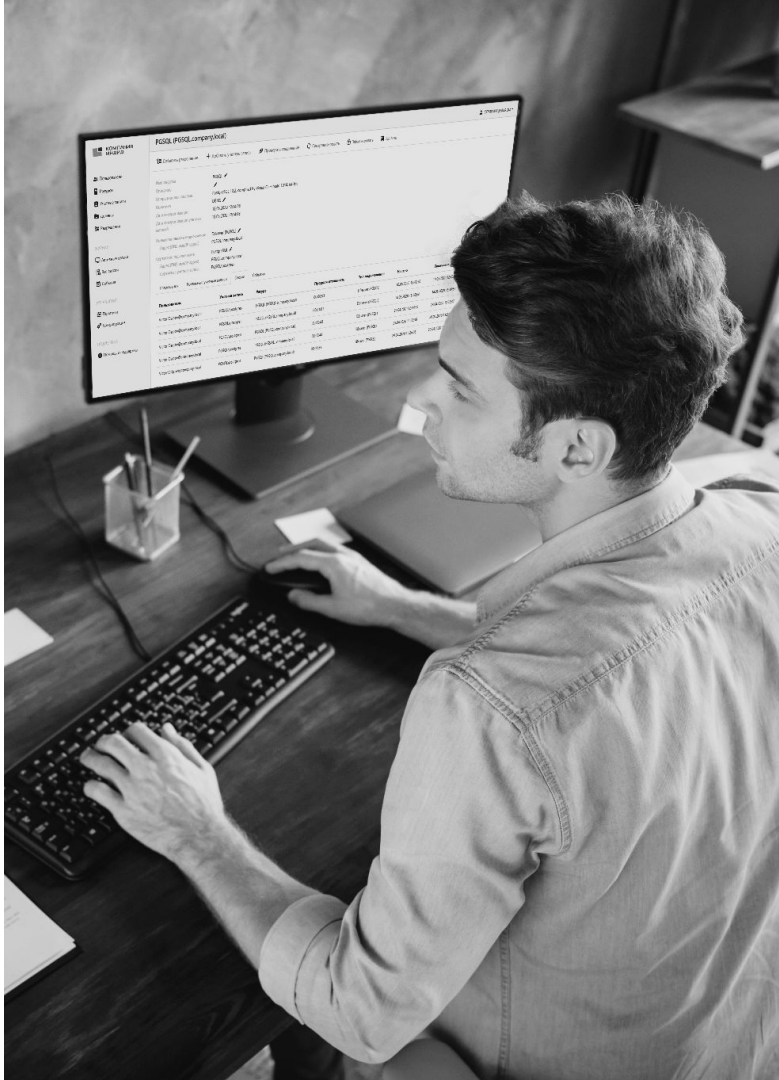
Единая система управления доступом
Инструменты для оптимизации подключения
Оценка объема работ подрядчиков

Минимизация угроз доступа и кражи пароля

Управление паролями учетных записей
Защита от несанкционированного обхода PAM
Доступ по согласованию и по расписанию
Встроенная двухфакторная аутентификация

Повышение производительности труда

Контроль и фиксация действий пользователей
Инструменты просмотра действий
Онлайн-передача событий и текстового лога в SIEM



КОМПАНИЯ
ИНДИД

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

КОМПАНИЯ
ИНДИД

НАШИ ЗАКАЗЧИКИ

Газпром нефть	НОВАТЭК	РОСНЕФТЬ	Газпром	РОССЕТИ
ГТЛК	CARCADE Группа Газпромбанк Лизинг	СТС	МАГНИТ	О'КЕЙ
ВТБ	Альфа Банк	БАНК САНКТ-ПЕТЕРБУРГ	МТС	epk

КОМПАНИЯ
ИНДИД

КОНТАКТЫ

indeed-company.ru

sales@indeed-company.ru

8 800 333-09-06