FUDO | PAM

# Практика применения next-generation PAM-системы для противодействия современным вызовам ИБ в РК

Защита от кибератак:
- управление доступами,
- защита паролей,
- предотвращение и запись действий,
- поведенческий анализ для контроля личности

+ эффективная работа привилегированных пользователей

Максим Прахов
Territory Manager for CIS, APAC
Fudo Security

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

Gartner peerinsights™ 4.6/5

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

# FUDO - ЛИДЕР НА РЫНКЕ PAM-РЕШЕНИЙ ЦЕНТРАЛЬНОЙ АЗИИ

**+30%**

**YoY рост, #1 по кол-ву проектов в СНГ**

**>60**

**заказчиков в странах СНГ**

**20**

**наград, включая Cybersecurity Excellence Awards**

Gartner peerinsights™ 4.6/5

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

**Факты о Fudo:** 100% фокус на PAM, первый релиз выпущен в 2016 году на основе принципов: безагентский подход, простота освоения, кастомизируемый интерфейс, защищенная архитектура на базе **all-in-one** аплаенса, нативная работа с сетевым трафиком

**#1** по количеству проектов в Казахстане - более 35 заказчиков за 3 года, референсы в каждой отрасли!

**#1** Локальное представительство в г. Алматы (менеджер и инженер)

**#1** Пользовательский интерфейс доступен не только на русском, но также и на **казахском** языке!

FUDO SECURITY

**2013 год – крупнейшая утечка и публикация десятков тысяч TOP Secret документов ЦРУ выполнена техническим специалистом добровольно, по личным (идеалистическим) убеждениям**

*В то время мне не приходило в голову, что **степень моего доступа означала глубокую уязвимость** во всей системе выдаче доступов…*

*…документ был так глубоко засекречен – всякий, кто имел к нему доступ, был немедленно идентифицирован, если только он не **системный администратор…***

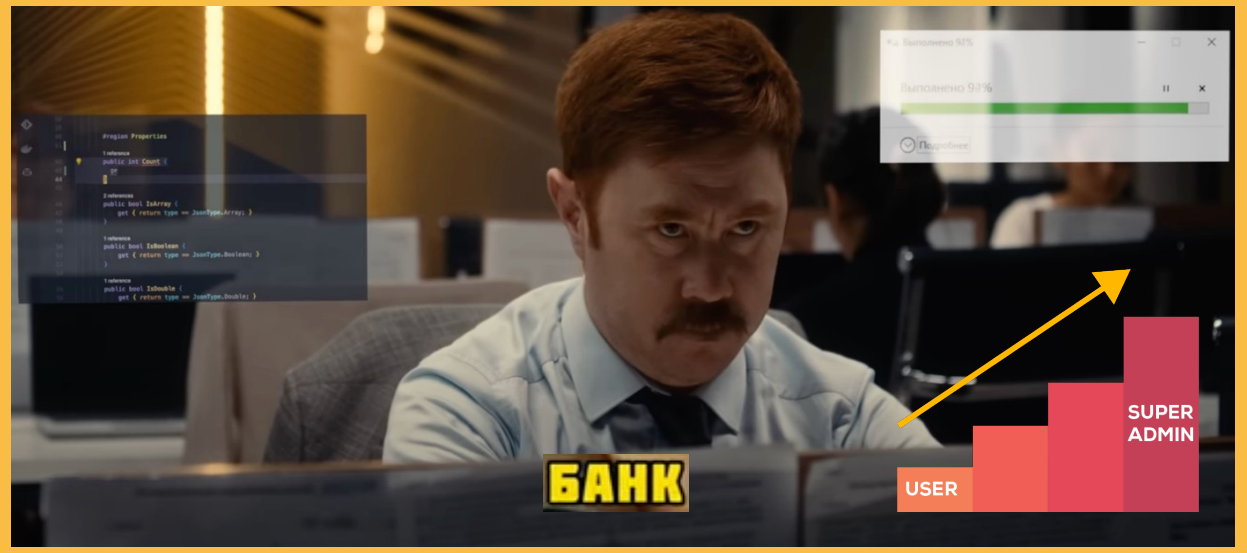
«Личное дело» Эдвард Сноуден

FUDO SECURITY

# Сериал Мошенники – основано на реальных событиях

## Может ли «простой инсайдер» обеспечить 3000 контактов/день для работы «call-центра»?



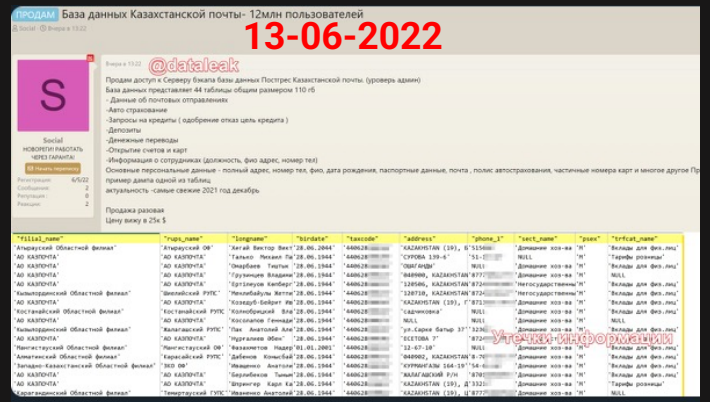



**Нужен привилегированный пользователь**

FUDO SECURITY

# Современные угрозы в Республике Казахстан

## Хронология инцидентов на основе данных тг-канала «Утечки Информации»




13-06-2022

На продажу выставлен доступ к серверу с резервной копией базы данных Почты Казахстана (*АО «Казпочта»*).

Со слов продавца в базе (*PostgreSQL*) 110 Гб информации и около 12 млн записей,

В открытый доступ был выложен дамп базы данных зарегистрированных пользователей предположительно онлайн-кинотеатра *«СТАРТ»* (*start.ru*). 🔥🔥

28-08-2022

Дамп в *JSON*-формате (получен вероятно из *MongoDB*) имеет размер 72 Гб и содержит информацию о 43,937,127 пользователях (включая тестовые записи):

- имя/фамилия (на русск. или англ. языках)
- адрес эл. почты (7,455,926 уникальных адресов)
- хешированный (частично *md5crypt*) пароль
- *IP*-адрес
- страна (24,6 млн из России, 2,3 млн из Казахстана, 2,1 млн из Китая, 1,7 млн из Украины)

Источник, который три дня назад "слил" данные внутренних пользователей (сотрудников) *«Билайн»*, выложил в открытый доступ информацию о сотрудниках розничной сети магазинов электроники *«DNS»* (*dns-shop.ru*). 👇

В текстовом файле 150,444 записи, из них 149,408 относятся к России и 1,036 - к Казахстану:

04-12-2022

- ФИО
- адрес эл. почты на доменах *dns-shop.ru*, *dns-shop.kz* и *dns.loc* (104,820 уникальных адреса)

Хакеры из проекта *Dark Slivki* заявили, что они получили доступ к данным зарегистрированных пользователей (представляющих компании из России, Украины, Казахстана и т.д.) рекомендательного сервиса *«Zoon»* (*zoon.ru*).

По нашей информации в полученных файлах содержатся:

28-09-2023

- имя
- название компании и должность
- телефон (около 400 тыс. уникальных номеров)
- адрес эл. почты (около 570 тыс. уникальных адресов)

В прошедшую субботу произошел массовый "слив" в открытый доступ множества баз данных, имеющих разное происхождение и актуальность, но являвшихся до этого дня "условно приватными" (этими базами активно обменивались, но они не были публично доступными). 🔥🔥

13-11-2023

Кроме того, в этом массовом "сливе" были замечены: *enbek.kz*


FUDO | PAM

# Вызовы кибербезопасности в 2023 году

Практически любая кибератака совершается через перехват/кражу/покупку админской (привилегированной) учетной записи!

**Эксперты выделяют рост числа атак через инфраструктуру внешних подрядчиков и поставщиков, т.к. их инфраструктура слабо защищена от кибератак!**

**Рост доли умышленных утечек – недобросовестные сотрудники активно ищут дополнительный заработок (в т.ч. привилегированные пользователи – владельцы данных)**

**Стоимость актуальной клиентской базы с контактными данными на рынке Darknet составляет 10-30 тыс. $, продажа совершается многократно!**

**Владелец БД знает как обойти агентский контроль DLP-системы, но не сможет обойти безагентский контроль и запись всех действий со стороны системы PAM**

**! ПРИМЕНЕНИЕ FUDO PAM КАРДИНАЛЬНО СНИЖАЕТ ДАННЫЕ РИСКИ !**

FUDO SECURITY

# Вызовы кибербезопасности - привычные практики ИТ

## Топ-5 проблем, которые мы обнаруживаем в компаниях в Казахстане:

1 **Администраторы сети регулярно открывают себе доступ к запрещенным ресурсам:**
Нарушения со стороны администраторов, например неправомерное изменение списков доступа на сетевом оборудование (чтобы открыть доступ до запрещенного сайта или для запрещенного приложения). Такие изменения могут затем годами оставаться в конфигурации оборудования.

2 **Использование одной учетной записи сразу несколькими администраторами:**
“Шарить” одну учетку между коллегами очень частая практика. Удобно, но после этого довольно сложно понять, кто именно ответственен за то или иное действие.

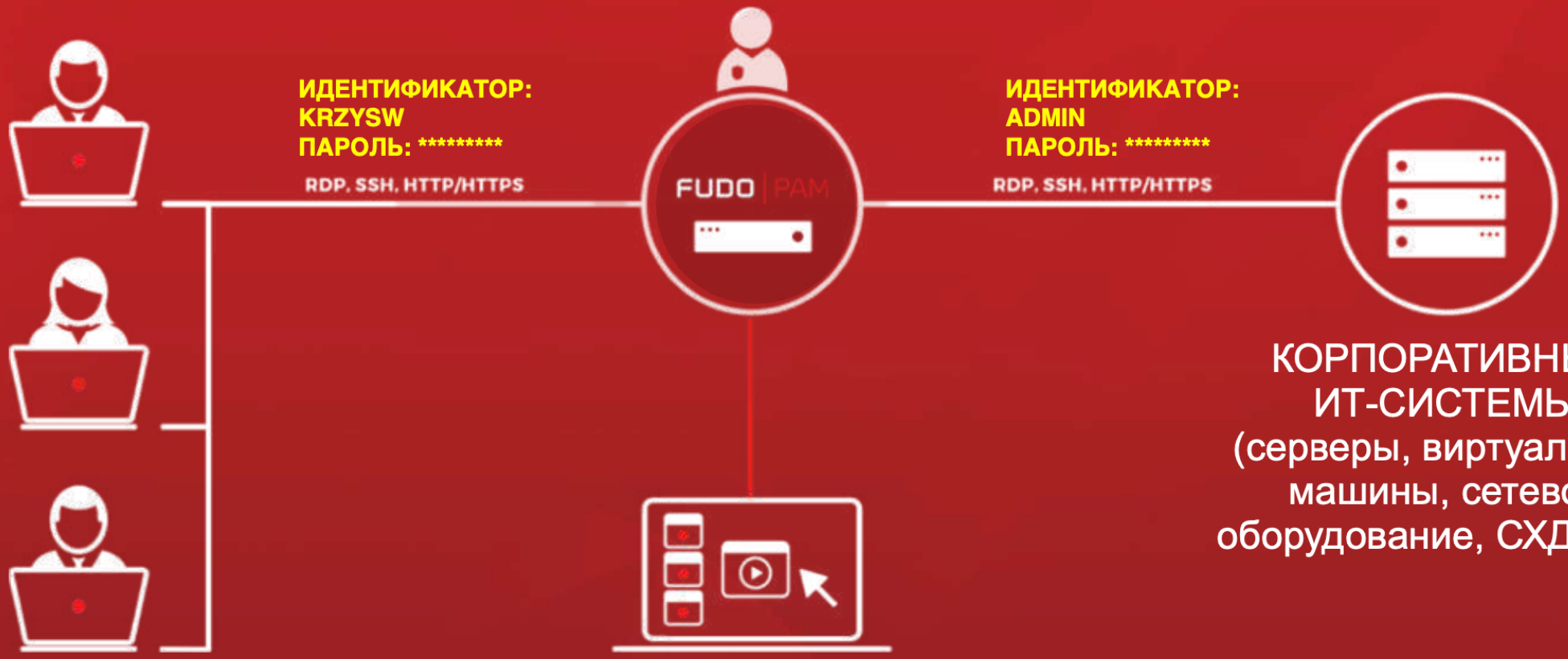
3 **Привилегированные пользователи скрывают следы ИТ и ИБ инцидентов:**
Реальный пример в компании РК: ИТ-администратор вечером нарушил работу важной ИТ-системы, с утра был срочно вызван в офис руководством для разбора всех обстоятельств, по пути на работу ИТ-администратор удалил все логи своей работы.

4 **Используется одинаковый пароль для множества систем:**
Запоминать несколько паролей всегда сложно - часто пользователи используют единственный пароль абсолютно для всех систем. Если такой пароль утечет, то злоумышленник получает доступ сразу ко многим системам.

5 **Пользователи обладают большими правами, чем предполагалось:**
Часто обнаруживается, что пользователи, с казалось бы урезанными правами, оказывается обладают бОльшими привилегиями (например могут перезагружать контролируемое устройство). Как правило это либо ошибка выдававшего права, либо просто недостатки встроенной системы разграничения прав.

FUDO SECURITY

# ПРИНЦИП РАБОТЫ FUDO PAM



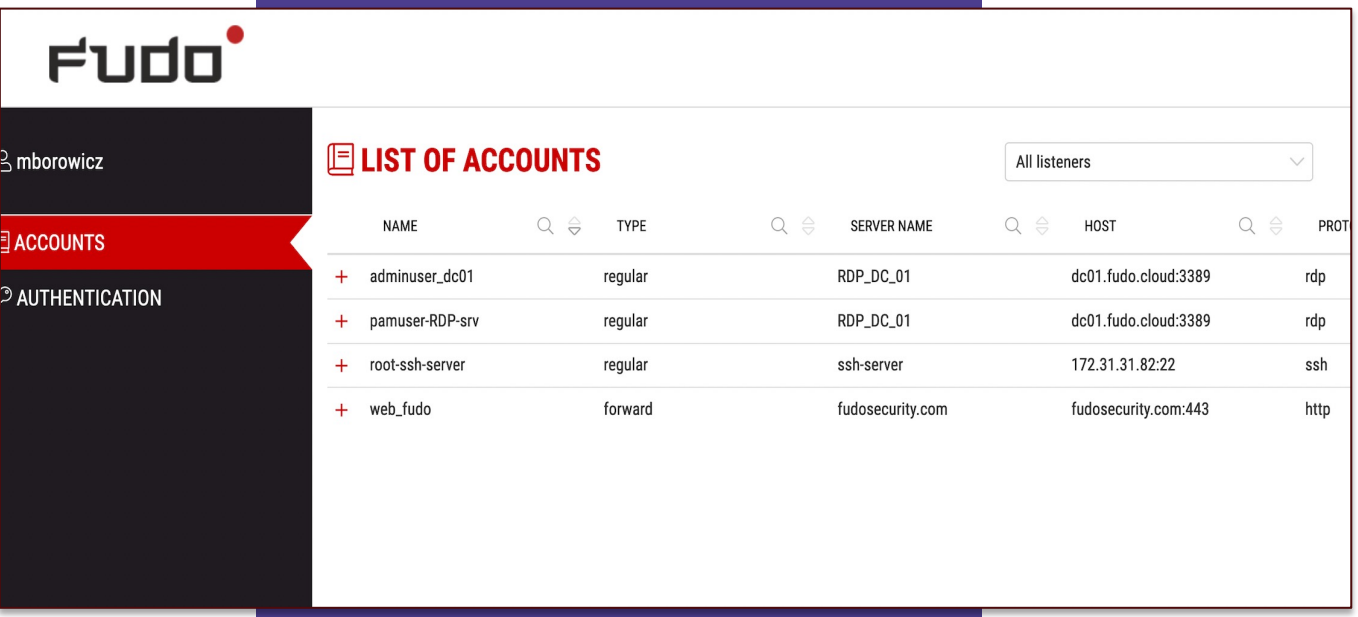

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ
(Администраторы ИТ, внешние подрядчики, разработчики и др.)

АДМИНИСТРАТОР FUDO
(рук-ль ИТ и/или специалист ИБ)
ПРОСМОТР РАБОТЫ И РЕАГИРОВАНИЕ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

КОРПОРАТИВНЫЕ ИТ-СИСТЕМЫ
(серверы, виртуальные машины, сетевое оборудование, СХД и др)

FUDO SECURITY

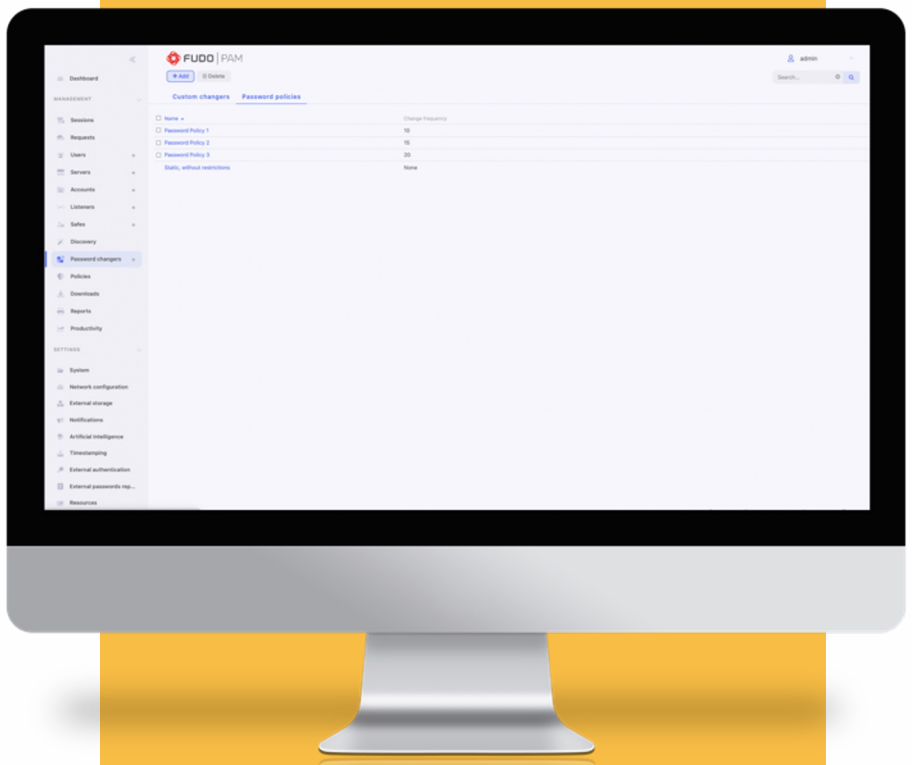
# Удобный веб-портал пользователя




- Единая точка входа (SSO) в рабочий кабинет со списком доступных рабочих сессий пользователя
- Автоматизация работы - не требуется ввод пароля для подключения к рабочей сессии с сервером
- Возможность организации совместной работы - генерация ссылки для подключения второго пользователя к сессии (с фиксацией действий)
- Подключение к сессиям через нативный или через web-клиент

FUDO SECURITY

# Полная автоматизация управления паролями на ИТ-системах



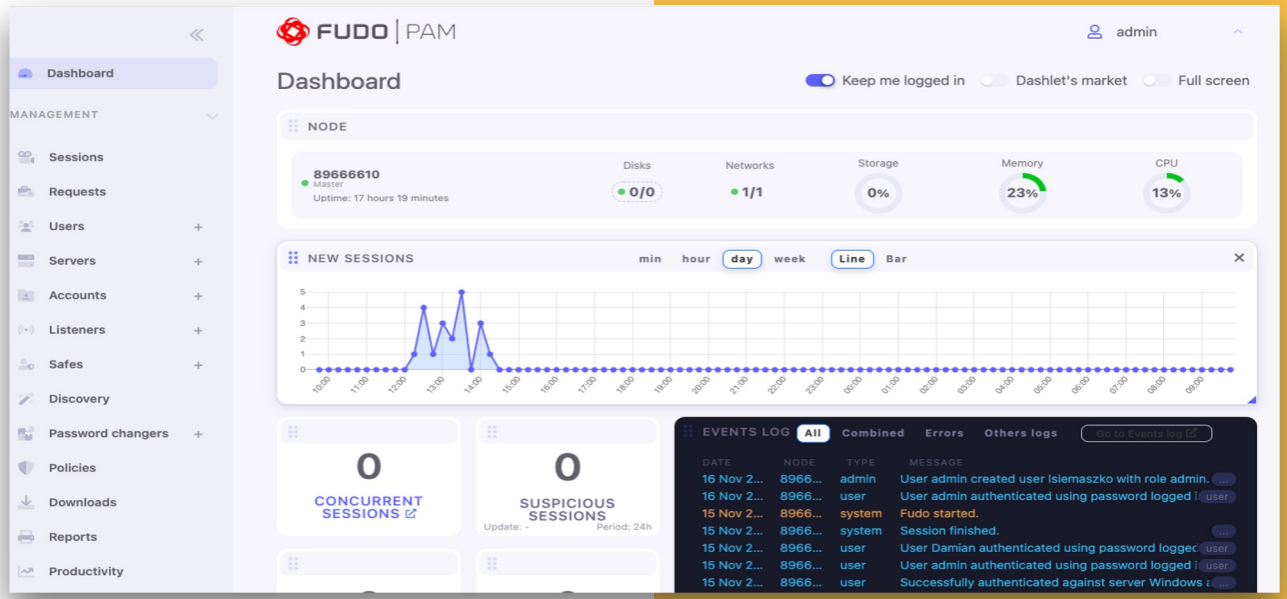

- ❏ Гибкая настройка частоты изменения паролей - возможность смены сразу после закрытия сессии
- ❏ Настройка требований к надежности пароля
- ❏ Безопасная доставка паролей в приложения, доступ через API и CLI
- ❏ Проверка смены пароля с помощью других механизмов
- ❏ История паролей позволяет восстановить пароль в случае стихийного бедствия или в целях восстановления
- ❏ Поддержка платформ: Unix, MS Windows, MySQL, CISCO

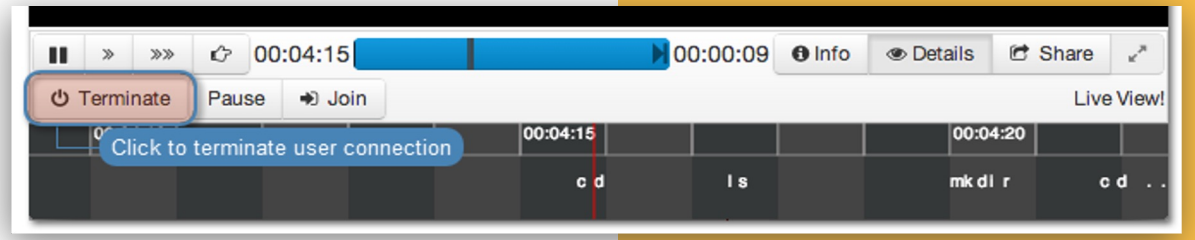
FUDO SECURITY

# Управление рабочими сессиями и мониторинг пользователей

## ШИРОКИЕ ВОЗМОЖНОСТИ КОНТРОЛЯ ДЛЯ АДМИНИСТРАТОРА FUDO

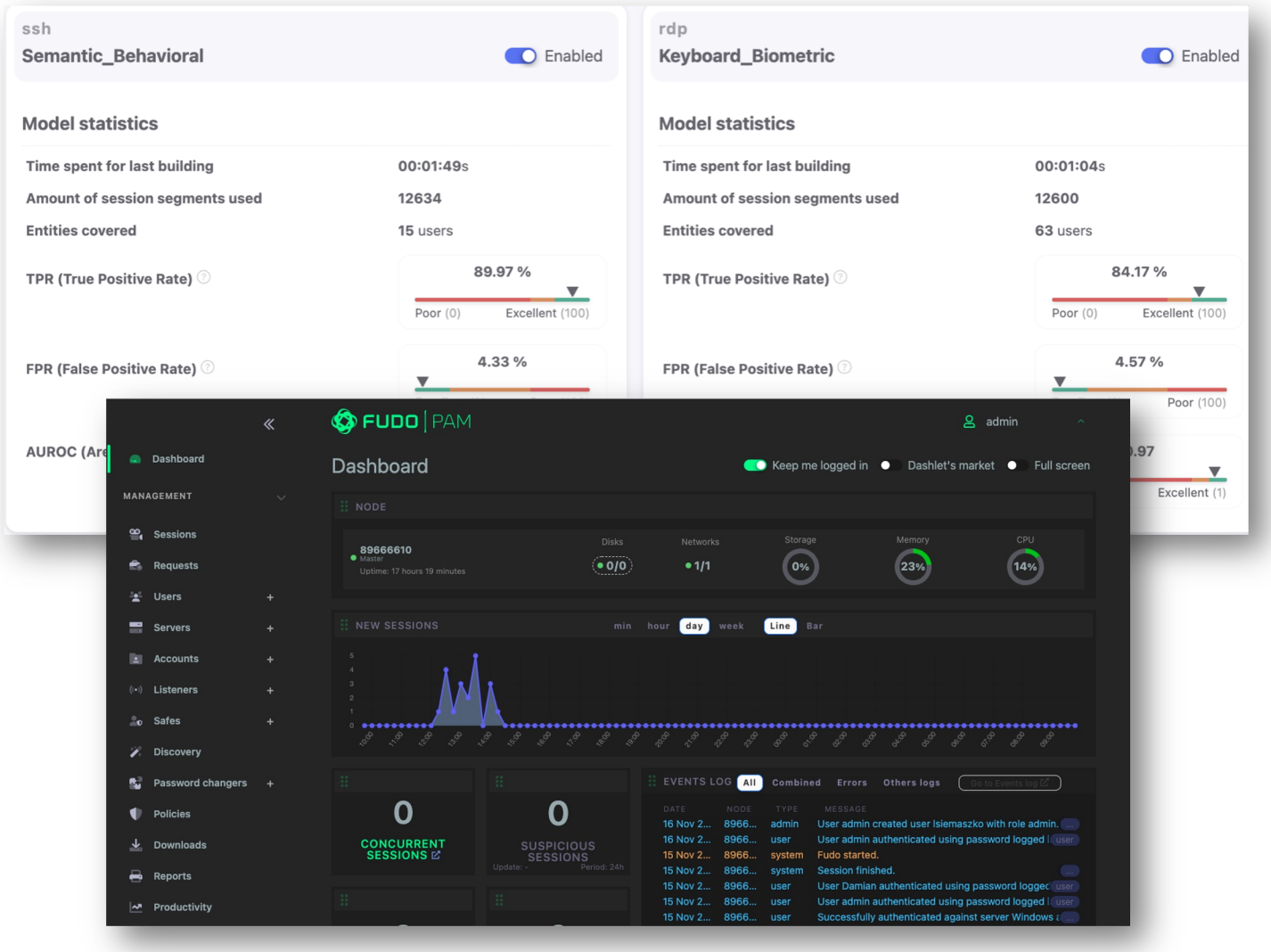
- ❑ Разбор сетевого трафика и контроль работы пользователей по протоколам: HTTP, HTTPs, Modbus, MS SQL(TDS), MySQL, RDP, SSH, Telnet, VNC, X11 & TCP + RemoteApp (Jump-host)
- ❑ Просмотр сессий «вживую» или записей через встроенный плеер
- ❑ Пауза, перехват, блокировка сессий
- ❑ Блокировка нежелательных команд на основе регулярных правил
- ❑ OCR-технология для распознавания текста, появившегося на экране пользователей - быстрый поиск по записям сессий




FUDO SECURITY

# Применение Fudo PAM для мониторинга и реагирования



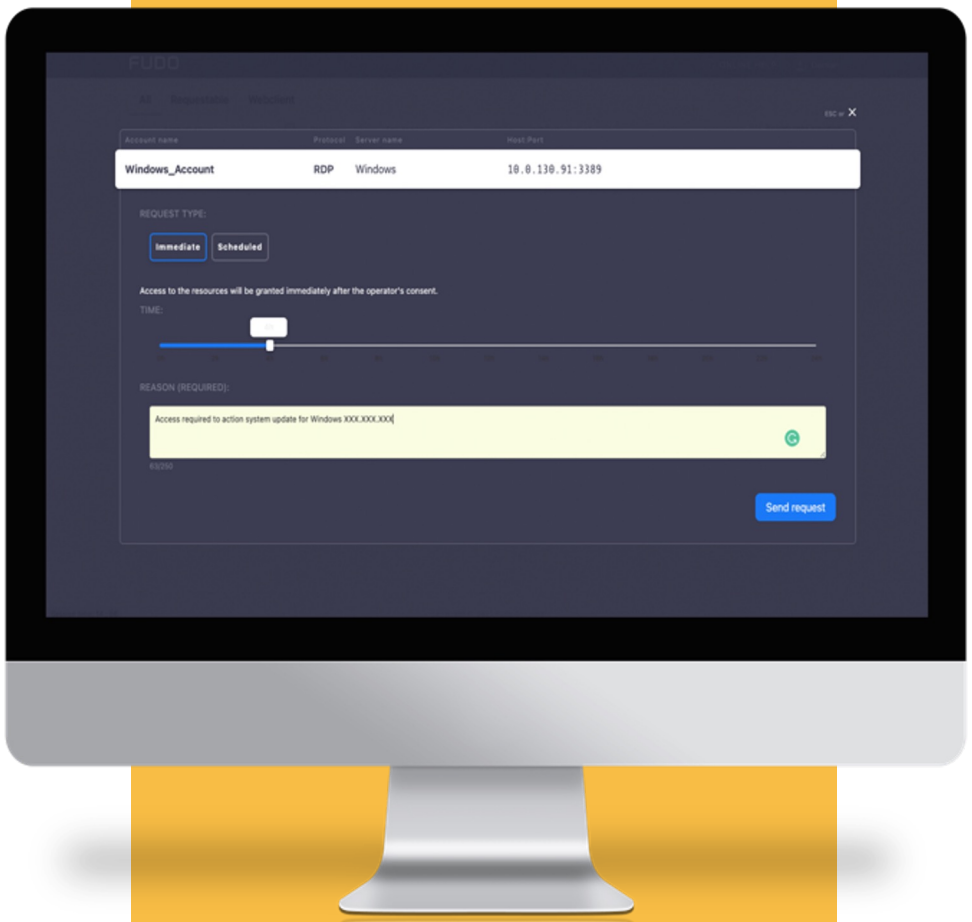

- **Поведенческий анализ (AI) на основе машинного обучения (ML) и контроля поведенческой биометрии** - возможность **менее чем за 60 секунд** выявить кражу или передачу привелигированной учетной записи третьим лицам!

- Начиная с релиза 5.3 - возможность автоматически заблокировать работу пользователя (сессию) в случае резкого отклонения в поведении!

- Улучшенный интерфейс - кастомизируемый дэшборд на HTML5, с возможностью выбора цветовых тем «Light», «Dark» и «Terminal

FUDO SECURITY

# Безопасный привилегированный доступ – временный доступ!

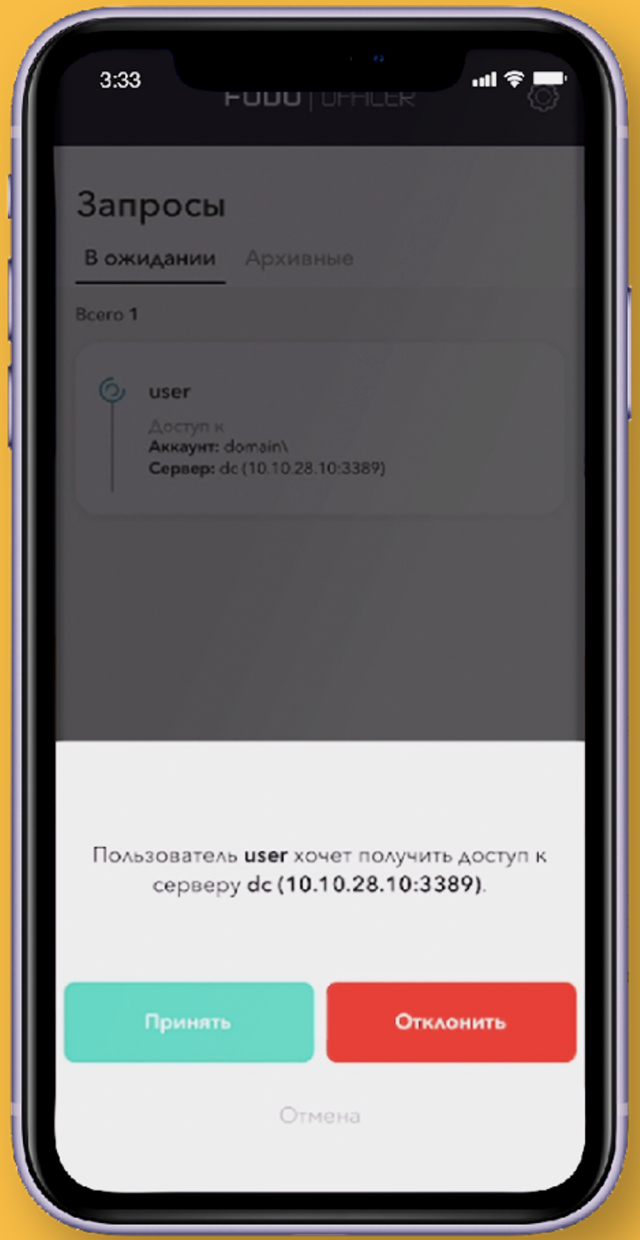



- Управление доступом в соответствии с концепцией Zero Trust (уход от постоянных/избыточных привилегий)
- Настройка гибких параметров временного доступа для пользователей, в т.ч. по расписанию или через API-интерфейс
- Портал самообслуживания - запрос доступа пользователями для одобрения администратором Fudo без необходимости задействования внешних систем

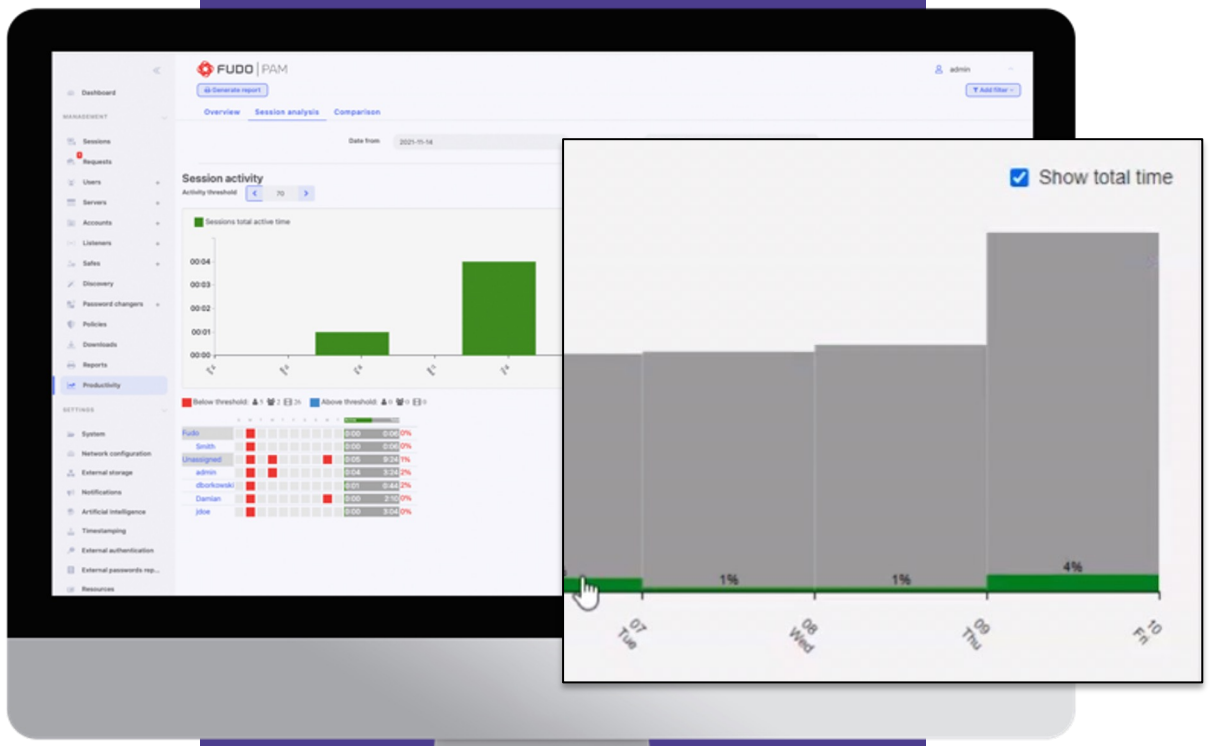
FUDO SECURITY

# Мобильное приложение Fudo Officer

- Быстрая обработка запросов пользователей на доступ при помощи мобильного телефона
- Поддержка нескольких профилей - можно управлять несколькими инстансами
- Защищенная авторизация в приложении с использованием Face ID,Touch ID или PIN-кода
- Бесплатно доступно на AppStore, подключение к серверу Fudo через QR-код
- Возможность указать причины отклонения запроса
- Фильтрация и поиск по архиву запросов



# Efficiency Analyzer - анализ продуктивности пользователей




- ❑ Графики времени активной работы в записанных сессиях за определенный период времени
- ❑ Возможность установки порога активности в % для наглядного анализа эффективности работы
- ❑ Возможность отобразить график с учетом общего времени запущенных сессий по отношению к активной работе в сессиях.
- ❑ Выгрузка графика в PDF, выгрузка видеозаписи рабочих сессий в MPEG/AVI с добавленными текстовыми метками-пояснениями

FUDO SECURITY

# Сценарии использования модуля анализа продуктивности


**Сокращение смет** внешних подрядчиков (окупаемость проекта Fudo за 3-6 месяцев)

**Понимание загруженности ИТ-команд**, планирование запуска новых проектов без переработок и сбоев ИТ

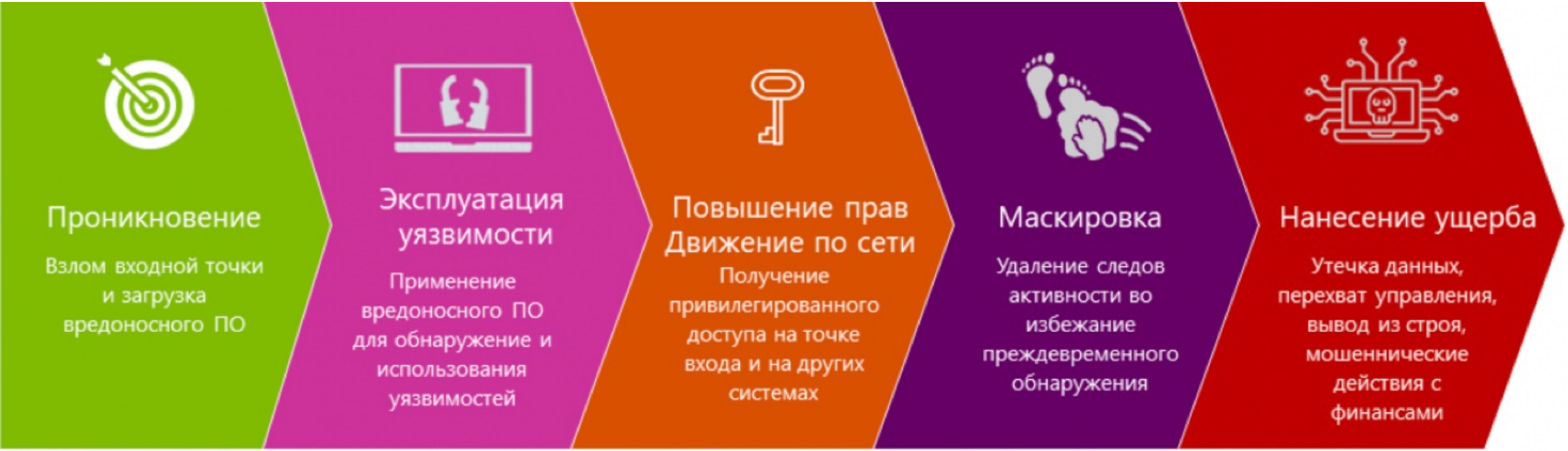
**Точный расчет переработок,** аргументация для поощрения перегруженных сотрудников

**ИБ - выявление аномальных** всплесков активности пользователей

**Повышение эффективности** работы ИТ-команды или разработчиков (перераспределение нагрузки, в т.ч. за счет обучения по записям сессий)

FUDO SECURITY

# Обнаружение и предотвращение кибератак при помощи PAM




Простое внедрение и сопровождение решений класса PAM позволяет противостоять атакующим на всех этапах, делая взлом **дорогим и сложным!**

Применение PAM – стандарт безопасности и необходимость каждой компании в 2023 году!

FUDO SECURITY

# Конкурентные преимущества Fudo PAM

**Технологический подход и защищенность**

Запись сеансов на лету с нативной поддержкой протоколов RDP, SSH и HTTP(s) - запатентованная технология!

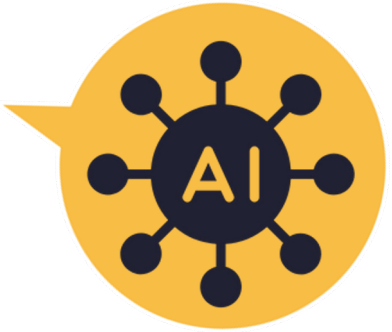
**Встроенный анализ продуктивности**

Модуль графического анализа и сравнения продуктивности работы пользователей/подразделений с возможностью выгрузки отчетов в формате PDF


FUDO SECURITY

**Быстрый запуск в работу, минимальные трудозатраты**

Комплексное решение - никаких агентов, никаких подключаемых модулей, настройки ОС или СУБД. Автоматизация добавления пользователей и эксплуатации




**Продвинутый поведенческий анализ (доступно on-premise!)**

Выявление аномалий и обнаружение взлома учетной записи менее чем за 60 секунд

# Основные сценарии применения FUDO PAM

Безопасная и эффективная работа с важными ИТ-системами

Безопасная работа и контроль действий подрядчиков и их смет (быстрая окупаемость)

Противодействие злоупотреблениям со стороны пользователей и быстрое расследование/реагировани

Возможность пользователям доказать корректность действий  или наоборот - доказательство вины

Управление паролями, общий доступ к учетным записям, автоматизация типовых задач

FUDO SECURITY

# Рахмет!

# Спасибо!

**Максим Прахов**

Региональный менеджер Fudo,
Страны ЦА и СНГ

+ 7 (778) 145 89 37

m.prakhov@fudosecurity.com

FUDO | PAM

Запуск пилотного тестирования за 1-2 часа!

(без необходимости дополнительного ПО или оборудования, требования: 4vCPU, 8GB RAM, 150GB HDD)

**Полное внедрение системы за 1-2 дня!**
**(включая обучение)**

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

Gartner peerinsights™ 4.6/5

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021