MULTIFACTOR ДиалогНаука

БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ ЗДЕСЬ

multifactor.ru

О компании

01

Компания МУЛЬТИФАКТОР

Наша миссия

Создание собственной экосистемы продуктов для безопасности ИТ-инфраструктуры заказчиков.

Компания

Сервис предоставляет ООО МУЛЬТИФАКТОР. Компания создана 9 декабря 2019 года и является на 100% российским юридическим лицом.

120+ партнеров

500+ успешных кейсов внедрения

30+ интеграций с российскими разработками и платформами

500 000 + пользователей системы (по итогам 2023 г.)

Команда опытных профессионалов

Кастомизация решения под бизнес-цели заказчика

Реагирование на инциденты **24/7**

Соответствие стандарту **PCI DSS**

Реестр отечественного ПО

Решение MULTIFACTOR находится в реестре российского ПО №7046.

Решение доступно бесплатно до трех пользователей

Подключить

Нам доверяют

О компании

ВКУСНО — И ТОЧКА

ВТБ

РЖД

DNS

О'КЕЙ

АЛРОСА

positive technologies

СБЕР ЛИЗИНГ

Ростелеком Солар

Demetra HOLDING

INVITRO

СУЭК
СИБИРСКАЯ УГОЛЬНАЯ ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

АЛЬФА СТРАХОВАНИЕ

РОССЕТИ
ФСК ЕЭС

AKRON HOLDING

TRANSMASHHOLDING

спортмастер

РОСВОДОКАНАЛ

Боли рынка

02

₽ 20 млн

Средний ущерб от кибератак хакеров для компаний в России [1]

14 млн

Россиян работают удаленно [2]

На 60%

Выросло количество утечек в мире за 2023 год [3]

> 4 млн записей ПДн

Приходится в среднем на одну утечку информации.

В 2022 году в результате одной утечки в среднем было скомпрометировано 2,98 млн записеи ПДн, то в 2023 году — 4,04 млн записеи, то есть произошел рост на 35,6% [3]

В результате компании сталкиваются с:

- прямым и косвенным финансовым ущербом;
- ущербом репутации и потерей клиентов;
- кражей интеллектуальной собственности и коммерческой тайны;
- санкциями от регуляторов за несоблюдение нормативных требований.

[1] По данным исследования «РТК-Солар» за 2023 г.

[2] По данным онлайн-опроса ВЦИОМа на 2022 г.

[3] По данным аналитического отчета InfoWatch: «Утечки информации в мире, 2022-2023 годы»

Цель атак злоумышленников – получение конфиденциальной информации

> 51%

Успешных атак методом социальной инженерии [1]

> 53%

Встречается проблема слабых паролей [2]

Основные каналы атаки:

- фишинговые письма;
- мессенджеры;
- телефонные звонки

Основные ассоциации при создании пароля:

- ФИО себя/родственников/домашнего животного;
- дата рождения

[1] По данным исследования «Positive Technologies» за 1 квартал 2024 г.

[2] По данным исследования «РТК-Солар» за 2023 г.

Проблемы

Небезопасность удалённых подключений

- Текущая геополитическая ситуация в стране, санкции, информационная война, хакинг, вирусы, фишинг и другие векторы атаки указывают на то, что пароли недостаточны для адекватной защиты.
- Подключения к ресурсам организации со скомпрометированных аккаунтов.
- Не отозванные доступы при увольнении сотрудника.

Неэффективные процессы управления доступом

- Результат простоя бизнес-процессов из-за нерешённых проблем с доступом — значительные финансовые и временные издержки.
- Высокая нагрузка на команду IT-поддержки в связи с онбордингом и офбордингом пользователей, организацией удалённого доступа, обслуживанием учетных записей, сменой забытых паролей и паролей с истёкшим сроком действия.

Реализация киберриска — вопрос времени, если превентивно не принять мер защиты подключении к корпоративным ресурсам.

Решение

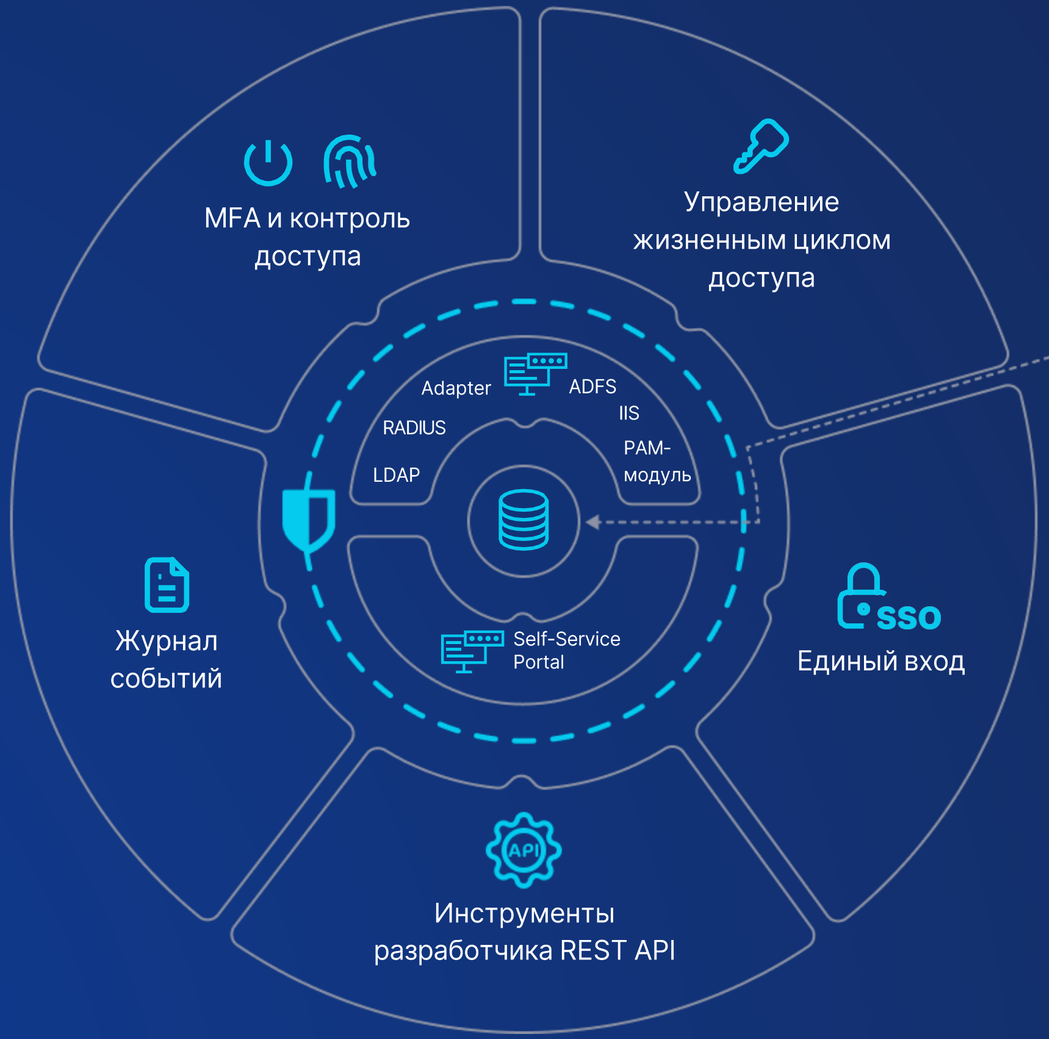
03

MULTIFACTOR

Сотрудники

Партнёры

Клиенты



Провайдер учётных записей

- MultiDirectory – LDAP-каталог УЗ от МУЛЬТИФАКТОР
- Active Directory
- Linux Astra Directory
- NPS
- Samba 4
- Freeipa

✓ Защита входа ✓ Простая интеграция ✓ Покрытие всей инфраструктуры

Отечественные и зарубежные VPN-шлюзы

- UserGate
- C-Терра
- КриптоПро NGate
- Континент 4
- Ideco UTM
- Рубикон
- CheckPoint
- Cisco
- FortiGate
- Mikrotik
- OpenVPN

Linux

- SSH
- SUDO
- OpenVPN
- PAM
- и др.

Windows

- Windows Logon
- VPN
- RD Gateway
- NPS
- и др.

SIEM-системы

- MULTIFACTOR совместим с SIEM-системами благодаря поддержке стандартных протоколов.

Облачные приложения, виртуализация, web

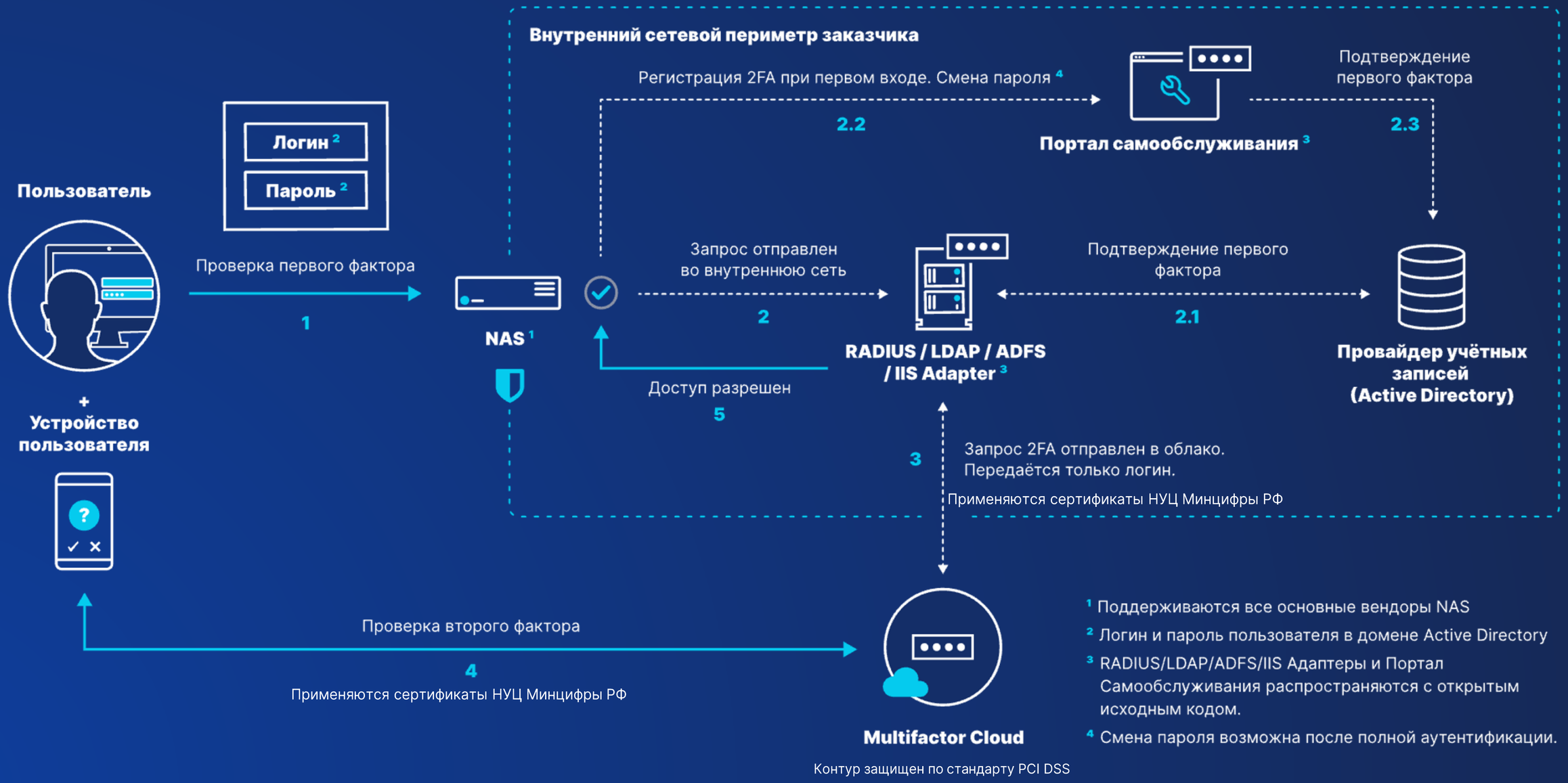
- SAML
- OIDC
- OAuth-приложения
- Мобильные приложения
- Outlook Web Access (OWA)
- VMware
- Huawei Cloud
- Яндекс.Облако
- Веб-сайты
- и др.

VDI

- VMware Horizon
- Citrix
- Remote Desktop
- и др.

Другое ПО

- СКДПУ АйТи-Бастион
- 1С-Bitrix24
- Точки доступа Wi-Fi
- и др.



[1] Поддерживаются все основные вендоры NAS

[2] Логин и пароль пользователя в домене Active Directory

[3] RADIUS/LDAP/ADFS/IIS Адаптеры и Портал Самообслуживания распространяются с открытым исходным кодом.

[4] Смена пароля возможна после полной аутентификации.

1 Компоненты On-Premise

1. Портал самообслуживания

- Самостоятельная регистрация сотрудником второго фактора аутентификации в Multifactor Cloud;
- Смена пароля в корпоративном домене Active Directory с обязательной проверкой текущего пароля и подтверждением вторым фактором в Multifactor Cloud;
- Компонент поставляется с открытым исходным кодом для Windows и для Linux

Мин. системные требования для Windows:

1 ядро CPU | 2Gb RAM | Windows Server 2012 и выше

Мин. системные требования для Linux:

1 Linux-сервер, протестирован на Debian 11

2. RADIUS, LDAP, ADFS, IIS Адаптеры

- Приём запросов на аутентификацию сотрудника в CheckPoint VPN, RDP и Citrix по протоколам;
- Проверка первого фактора аутентификации (логин и пароль) в домене;
- Проверка второго фактора аутентификации в Multifactor Cloud;
- Компоненты поставляются с открытым исходным кодом для Windows и Linux.

Мин. системные требования для Windows:

4 ядра CPU | 4Gb RAM | Windows Server 2012 и выше

Мин. системные требования для Linux:

1 CPU | 2 GB RAM | 8 GB HDD

2 Облако Multifactor

multifactor.ru

Безопасное размещение в ДЦ DataLine, Selectel и Yandex Cloud

- Подтверждение и подпись запросов на аутентификацию пользователей вторым фактором;
- Личный кабинет IT-службы вашей организации для управления и контроля доступа сотрудников к ресурсам с 2FA;
- Журнал событий;
- API и инструменты разработчика.

SLA

- Аптайм **99.99%**
- Тех. поддержка

Обзор технологии MFA

04

Мультифакторная аутентификация

Пользователи могут подтвердить свою личность тем, что они знают (основной метод аутентификации, как правило, логин и пароль); тем, что у них есть (например, аппаратный или программный токен); тем, кем они являются (биометрия). Последние два — возможные способы проверки второго фактора.

1

Первый фактор

Что пользователь знает?

Логин и пароль

2

Второй фактор

Что пользователь имеет или кем является?

Telegram

Звонок

Приложение

SMS

Токен (OTP, FIDO[1], U2F[1])

Биометрия[1]

3

Доступ

Доступ разрешён

[1] FIDO, U2F токены и биометрия недоступны в конфигурации с межсетевыми экранами NAS (Checkpoint, Cisco, Mikrotik и др.) и VDI.

Поддерживаемые методы аутентификации

В таблице представлены 6 основных методов проверки второго фактора, поддерживаемых MULTIFACTOR, в зависимости от сценария использования.

	VPN и VDI	Linux инфраструктура	Windows инфраструктура	Облачные приложения (SAML)	API (Web)
Мобильное приложение Multifactor	✓	✓	✓	✓	✓
Telegram-бот Multifactor	✓	✓	✓	✓	✓
SMS или звонок	✓	✓	✓	✓	✓
OTP токены (Аппаратные и программные)	✓	✓	✓	✓	✓
U2F / FIDO токены				✓	✓
Биометрия				✓	✓

Портал самообслуживания
Self-Service Portal (SSP)

05

Портал самообслуживания для пользователей Active Directory и других LDAP-каталогов

Позволяет пользователю самостоятельно настраивать и подтверждать владение вторым фактором доступа, менять текущий, истекший или забытый пароль после полной аутентификации. Управление устройствами Exchange ActiveSync. Подробнее о портале на сайте

Самостоятельный онбординг пользователей

2FA

Самостоятельная конфигурация 2FA

Возможность самостоятельного восстановления забытых паролей пользователями Active Directory (при условии прохождения предварительной аутентификации в мобильном приложении Multifactor)

Решение проблем с доступом без участия IT-поддержки

Компонент поставляется с открытым исходным кодом для Windows и Linux.

Мин. системные требования:

- 1 ядро CPU
- 2Gb RAM
- Windows Server 2012 и выше

Обзор технологии Единый вход (SSO)

06

Управление парком облачных приложений в современной компании стало большой проблемой

С ростом организации растет и количество кусочков технологического пазла: все больше приложений, пользователей и устройств — в различных географических локациях. Команды IT и безопасности должны обеспечить доступ к приложениям для защиты корпоративных данных, одновременно упрощая этот доступ для сотрудников, которым необходимо сохранять продуктивность.

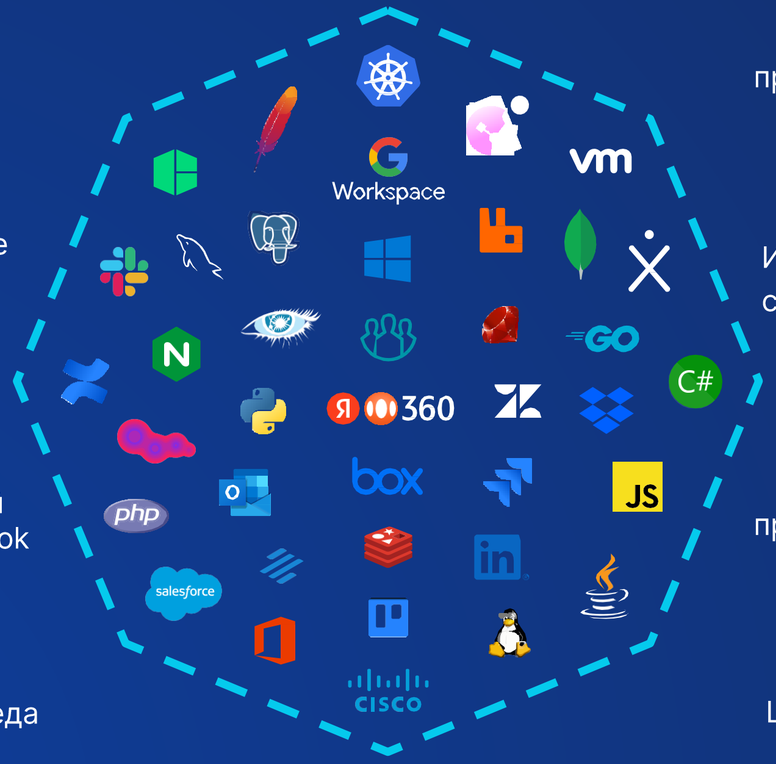
Технологический пазл

Облачные приложения

Собственные приложения

OWA и мобильный клиент Outlook

Windows-среда



SAML 2.0 приложения

Интеграция с Keycloak

Веб - приложения

Linux-среда

Проблемы

1 Затраты на поддержку

- Мультипликация учётных данных в облачных сервисах и системах идентификации.
- Трата ресурсов на неэффективный онбординг и офбординг пользователей ответственными сотрудниками.

2 Угрозы безопасности

- Не отозванные доступы сотрудников.
- Безопасность учётных данных и подключений.

3 Продуктивность сотрудников

- Запоминание паролей, их учёт, соответствие различным парольным политикам, необходимость использовать сторонние инструменты (аппаратные токены, VPN) отнимает силы у рядовых работников.

SSO MULTIFACTOR — упрощение контроля доступа к корпоративным приложениям и второй фактор

Уменьшение затрат

Единый провайдер учётных записей позволяет легко управлять всеми пользователями организации, выдавая доступы в зависимости от должности.

Улучшенный пользовательский опыт

Отпадает необходимость запоминать множество паролей и учётных записей. Возможность изменения паролей во всех сервисах в пару кликов.

Лучшее соответствие требованиям безопасности

Внедрение второго фактора во все системы, вне зависимости от их возможностей.

Настраиваемые парольные политики

Парольные политики зависят от провайдера учётных записей, а не от сторонней системы.

Увеличенная продуктивность

Упрощенный контроль за доступами пользователей. Простое управление перемещением человеческих ресурсов организации.

Упрощённая связность

Интеграция нового приложения в инфраструктуру компании занимает меньше времени.

Регистрация 2FA пользователями

07

1 Автоматическая регистрация

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Автоматическая регистрация СМС в качестве второго фактора доступа (синхронизация телефонных номеров с Active Directory).

2 Регистрация в режиме самообслуживания

✓ 1) Диалог с пользователем Подробнее

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Технология позволяет настроить второй фактор в режиме диалога с пользователем непосредственно в VPN/VDI клиенте или в API/SAML интерфейсе MULTIFACTOR при первом подключении.

✓ 2) Портал самообслуживания Подробнее

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

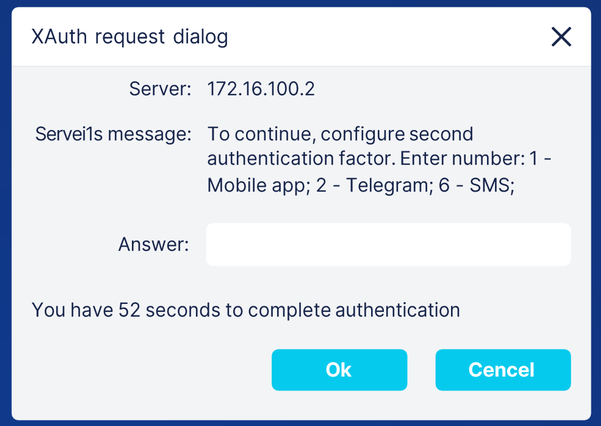
Портал позволяет настроить второй фактор в режиме самообслуживания. В этом сценарии необходимо подготовить и разослать пользователям инструкцию.

3 Регистрация вручную

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

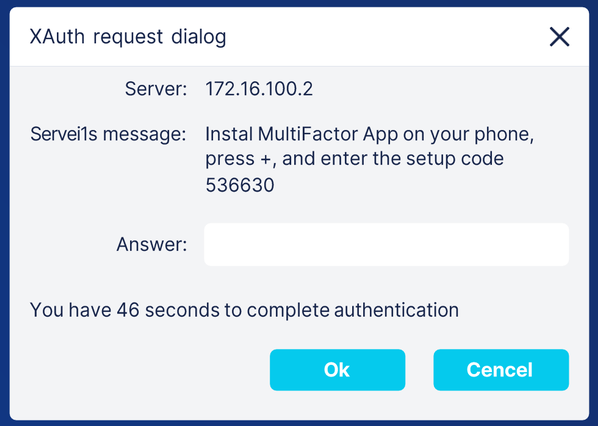
Администраторы вручную добавляют или импортируют пользователей и рассылают регистрационные ссылки на email.

1 Выбор фактора



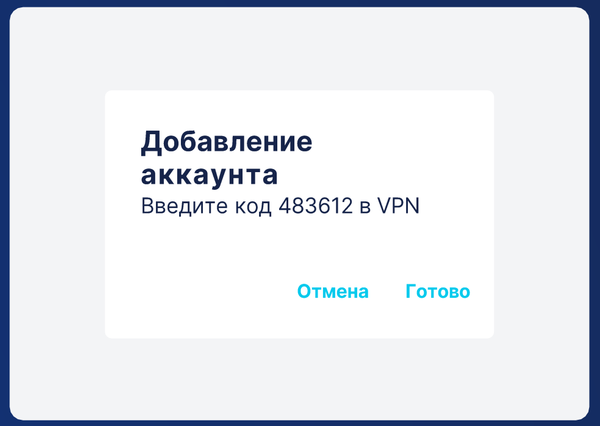
Пользователь выбирает удобный ему способ двухфакторной аутентификации из преднастроенного списка [1], вводя соответствующую цифру.

2 Привязка фактора



Клиент сообщает пользователю код, который ему необходимо ввести в приложении или Telegram-боте Multifactor.

3 Подтверждение владения



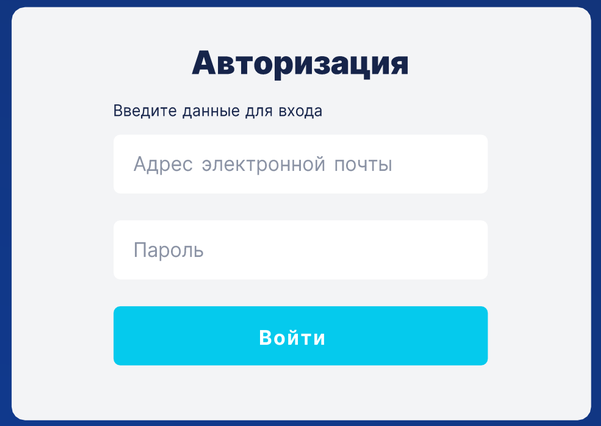
Пользователь подтверждает владение фактором, вводя код из Telegram, мобильного приложения Multifactor или СМС обратно в клиент.

4 Готово!

Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

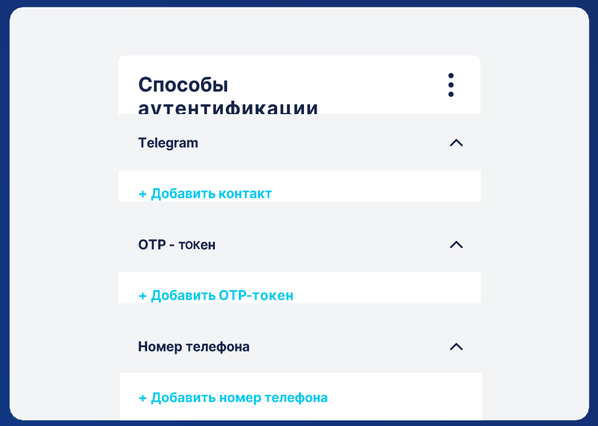
1 Telegram, СМС, Приложение Multifactor в случае защиты VPN и VDI соединений.

1 Первое подключение



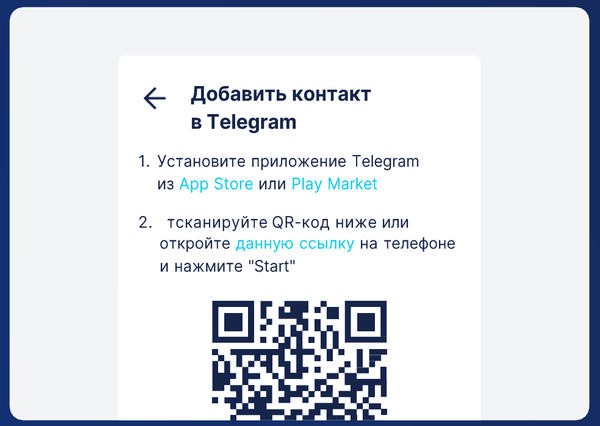
Пользователь проходит аутентификацию на Портале Самообслуживания (учетные данные Active Directory);

2 Выбор фактора



Пользователь выбирает удобный ему способ двухфакторной аутентификации из преднастроенного списка [1]

3 Подтверждение владения



Пользователь подтверждает владение фактором.

4 Готово!

Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

1 Telegram, СМС, Звонок, Приложение Multifactor или OTP-токены (аппаратные или программные) в случае защиты VPN и VDI соединений.
2 Например, в случае подтверждённой утери второго фактора или объективной невозможности использования второго фактора.

Почему MULTIFACTOR?

08

Высокая доступность

Аптайм 99.98% времени. Решение, проверенное реальными интеграциями с клиентами.

Отказоустойчивость

Отказ облака Multifactor не скажется на вашем бизнесе. В худшем случае инфраструктура возвращается на предыдущий уровень доступа, без использования второго фактора.

Производительность

Облако Multifactor — 1800 tps; RADIUS Adapter - 120 tps [1]

Безопасность инфраструктуры

Облако Multifactor располагается в дата-центрах DataLine, Selectel, Yandex Cloud в Москве с многоуровневой физической защитой, резервными интернет-каналами и источниками питания.

Масштабируемость

Без ограничений по количеству пользователей и ресурсов.

Нулевой CAPEX

SaaS решение для любого бизнеса.

Простая адаптация пользователей

Интуитивный и простой процесс подключения пользователей к многофакторной аутентификации. Возможность автоматического подключения.

Упрощение работы пользователей

MULTIFACTOR позволяет упростить парольные политики. Комбинируется с возможностями SSO.

Настройка любых процессов

Возможность добавить любую необходимую бизнес-логику.

Режим ByPass

Позволяет группам или отдельным пользователям входить без второго фактора

SLA

- Аптайм **99.99%**
- Реагирование на инциденты **7x24x1H**

[1] Горизонтальное масштабирование при необходимости

Создаем несколько уровней добавленной ценности

Ценность для руководства

CEO

Выстраивание доверия с различными сторонами: клиентами, партнёрами, инвесторами, потребителями, регулирующими органами;

Повышение устойчивости бизнеса.

CFO

Доступное решение для управления киберриском;

Оптимизация резервов под киберриск;

Защита критической информации;

Прогнозирование спроса на лицензии.

COO

Непрерывность рабочих процессов;

Координация предоставления доступов;

Управление процессом найма и увольнения сотрудников.

CSO and CIO

Безопасность точек входа в инфраструктуру;

Повышение барьеров для злоумышленников;

Организация безопасности удалённой работы;

Оптимизация аудитов безопасности.

MULTIFACTOR

Подписывайтесь на наш официальный Telegram-канал

Наши соц.сети

@multifactor

/multifactor

Мы в TenChat

@multifactor_news

@multifactor9508

ДиалогНаука

Эксклюзивное предложение для участников вебинара!

Обратитесь к нам с зарегистрированной почты в течение двух недель и получите 10% скидки.

Для записи на консультацию пишите нам:
marketing@dialognauka.ru