MULTIFACTOR

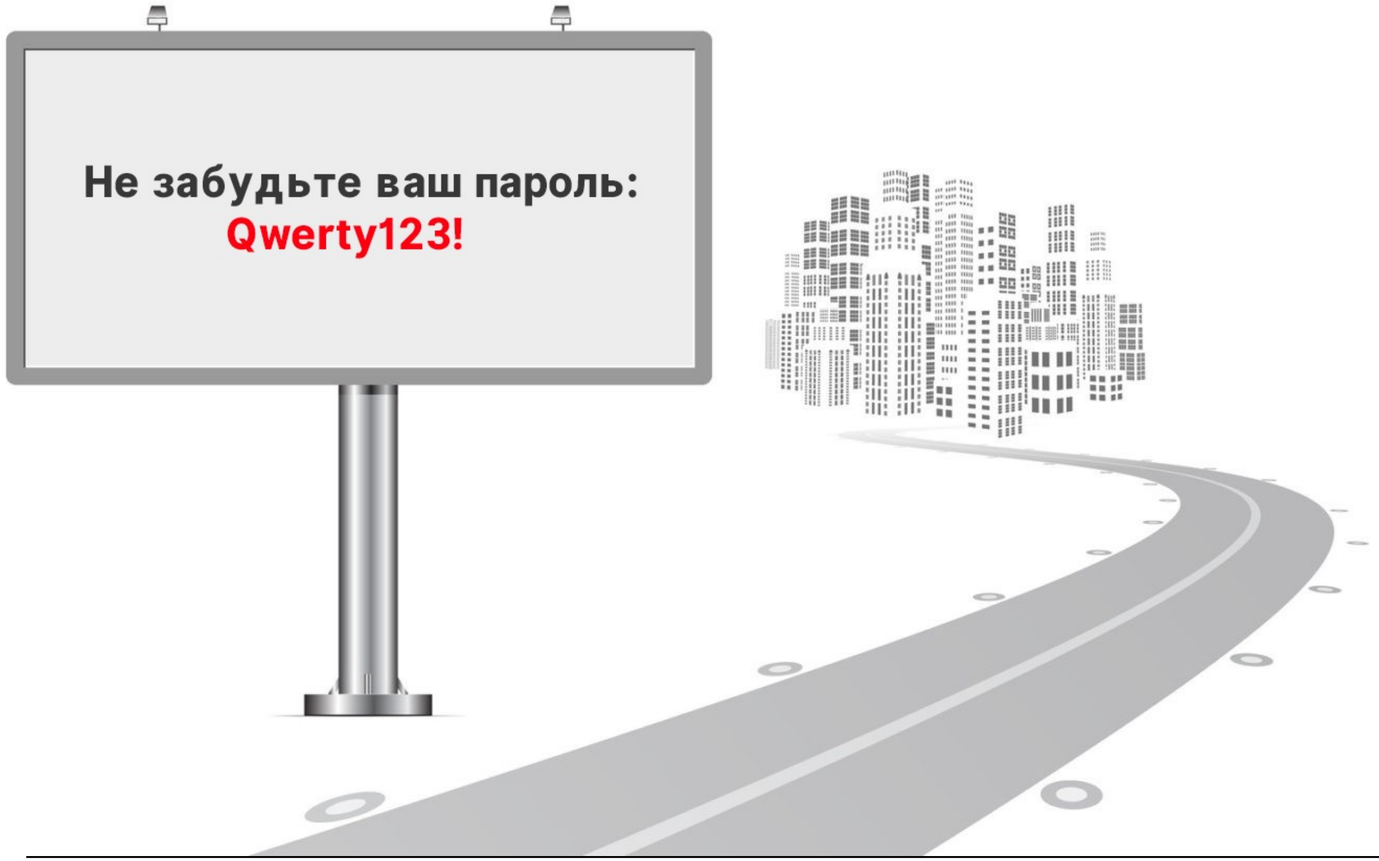
MULTIFACTOR: вчера, сегодня и навсегда

Роман Коротун
Директор по продажам

1. Боли рынка

Проблемы удалённого доступа

Обзор



₽ 60 000

Потери компаний в РФ в расчёте на сотрудника

Средний ущерб от кибератак для компаний в РФ[1]

[1] По данным отчета IBM Security за 2022 год

Обзор

8 млн

Человек в РФ работают дистанционно[1]

+ 45%

Количество утечек в Росси за 1-е полугодие 2022 г. по сравнению с 2021 г.[2]

230 млн

УЗ россиян утекло в сеть в 2022 году[3]

< 187 млн

Количество скомпрометированных записей в России за первое полугодие 2022 г. превысило население страны[2]

на 25%

Выросло кол-во атак на российские компании в 2022 году по сравнению с 2021 годом[4]

х 4 раза

выросло число кибератак на российские компании в первые месяцы 2022 г. по сравнению с аналогичным периодом 2021 г.[5]

[1] По данным АО "Эр-Телеком Холдинг" и Gartner
[2] По данным аналитического отчета InfoWatch за 1 половину 2022 г.
[3] По данным Роскомнадзора
[4] По данным аналитического отчета Positive Technologies за 2022 год
[5] По данным аналитического отчета «Индекс безопасности» от Мегафон

Обзор

Текущая геополитическая ситуация в стране, санкции, информационная война, хакинг, вирусы, фишинг и другие векторы атаки указывают на то, что пароли недостаточны для адекватной защиты.

Основная проблема возникновения внешних угроз – это незащищенность удаленных подключений.

В результате компании терпят:

- прямой и косвенный финансовый ущерб;
- ущерб репутации и потерю клиента;
- кражу интеллектуальной собственности и коммерческой тайны;
- санкции от регуляторов за несоблюдение нормативных требований.

$ 4,35 млн

Средний ущерб от кибератак для компаний в мире[1]

[1] По данным отчета IBM Security за 2022 год

2. Решение

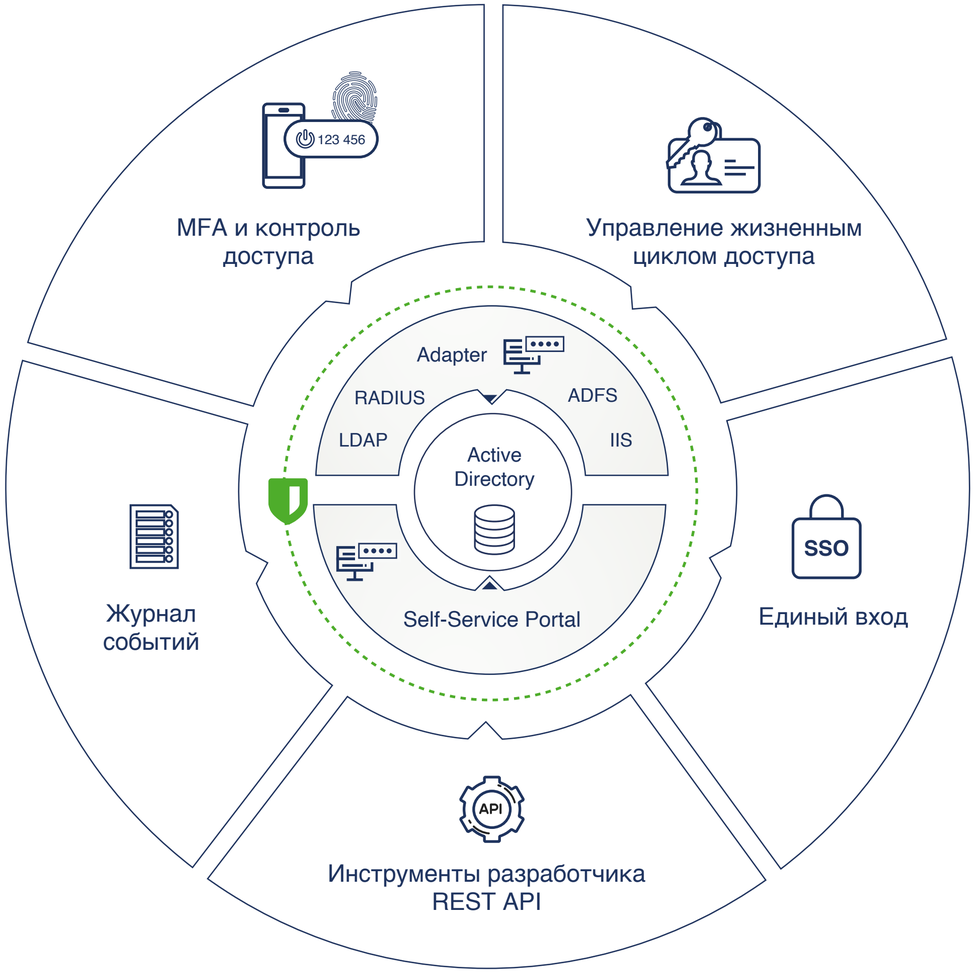
Продукт MULTIFACTOR

MULTIFACTOR с одного взгляда

Сотрудники

Партнёры

Клиенты



1. **VPN**
   CheckPoint, C-Teppa, Cisco, FortiGate, Mikrotik, OpenVPN, UserGate, Ngate, Континент и др.

2. **VDI**
   VMware Horizon, Citrix, Remote Desktop и др.

3. **Облачные приложения, виртуализация, web:**
   SAML, OIDC, OAuth-приложения, мобильные приложения, VMware, Huawei Cloud, Yandex Cloud и др. Веб-сайты, Outlook Web Access.

4. **Linux**
   Linux Logon, OpenVPN, SSH, SUDO и др.

5. **Windows**
   Windows Logon, VPN, RD Gateway, NPS, OWA, Remote Desktop и др.

✓ Защита входа

✓ Простая интеграция

✓ Покрытие всей инфраструктуры

Протоколы интеграции

- API
- RADIUS
- LDAP
- oAuth
- OpenID Connect

Защищаемые системы

- VPN и VDI
- Linux-инфраструктура
  (В том числе все российские дистрибутивы)
- Windows-инфраструктура
- WEB-приложения
- Облачные приложения
  (Как удаленный, так и локальный вход)
- Портал самообслуживания

Решение MULTIFACTOR

Продукт в [реестре российского ПО]();

CAPEX
0₽

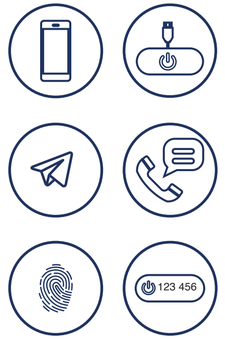
Не требует затрат на внедрение и инфраструктуру.

от
2 часов

Интеграция и ввод в эксплуатацию.
Быстрый онбординг.

до
99%

Снижение рисков неавторизованного доступа **без создания новых.**



MFA и контроль доступа

- Безопасность доступа к инфраструктуре;
- Предотвращение угонов учетных записей, утечек данных и сетевых атак;
- Защита VPN и VDI-подключений;
- Защита облачных SAML-приложений;
- Защита Windows и Linux инфраструктуры.

Портал самообслуживания

- Самостоятельный онбординг пользователей
- Самостоятельная конфигурация 2FA;
- Решение проблем с доступом без участия IT-поддержки (включая смену просроченного пароля).

Единый вход и Управление доступом

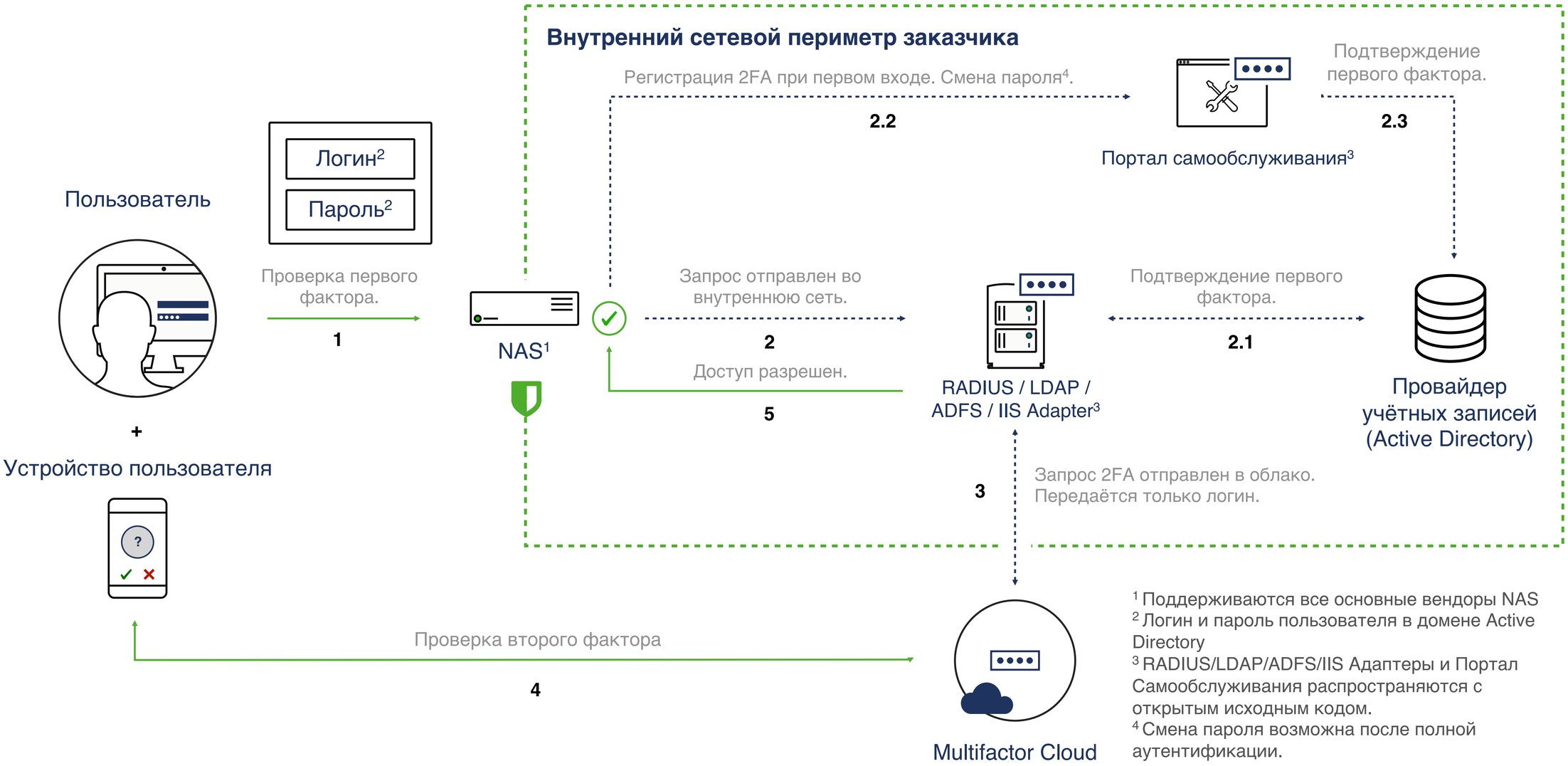
- Исключает мультипликацию учётных записей в облачных системах;
- Единый поставщик учётных записей для доступа к вашим приложениям;
- Упрощает приём на работу и увольнение сотрудников для IT.

✓ **Безопасность**
Дополнительный уровень защиты поверх ваших основных методов аутентификации.

✓ **Снижение затрат на поддержку**
Упрощение разрешения проблем с доступом.

✓ **Непрерывность процессов**
Интуитивный UX, повышение продуктивности сотрудников.

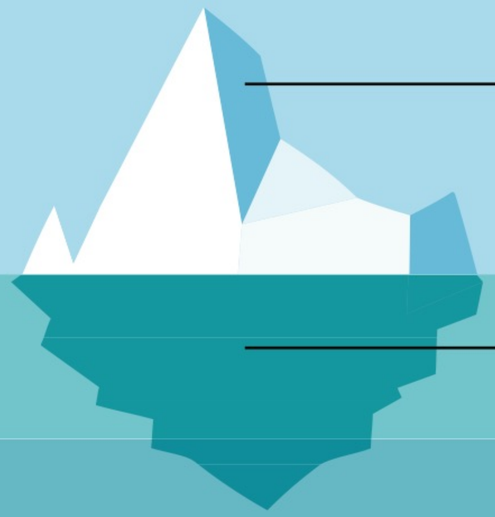
Высокоуровневая схема решения



[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.

ПОЧЕМУ МУЛЬТИФАКТОР?

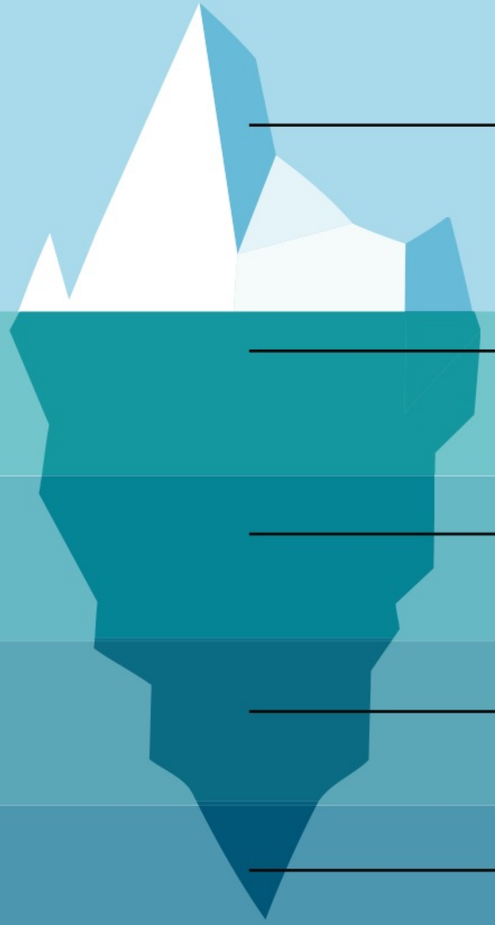
MULTIFACTOR SAAS



Стоимость подписки

Внедрение, настройка и обучение

ON-PREMISES РЕШЕНИЕ



Стоимость лицензирования программного обеспечения

Внедрение и настройка

Серверное оборудование, токены

Ресурс ИТ-подразделения

Обучение

ТЕКУЩИЕ РАСХОДЫ

Стоимость подписки / Обучение / Настройка

ТЕКУЩИЕ РАСХОДЫ

Обновление ПО / Постоянная нагрузка на ИТ / Простой / Обновление и поддержка серверов / Оптимизация производительности / Обновление зависимостей / Перепрошивка токенов / Поддержка и обновление

4. Обзор технологии

Единый вход (SSO)

Управление парком облачных приложений в современной компании стало большой проблемой

С ростом организации растет количество кусочков технологического паззла: 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.

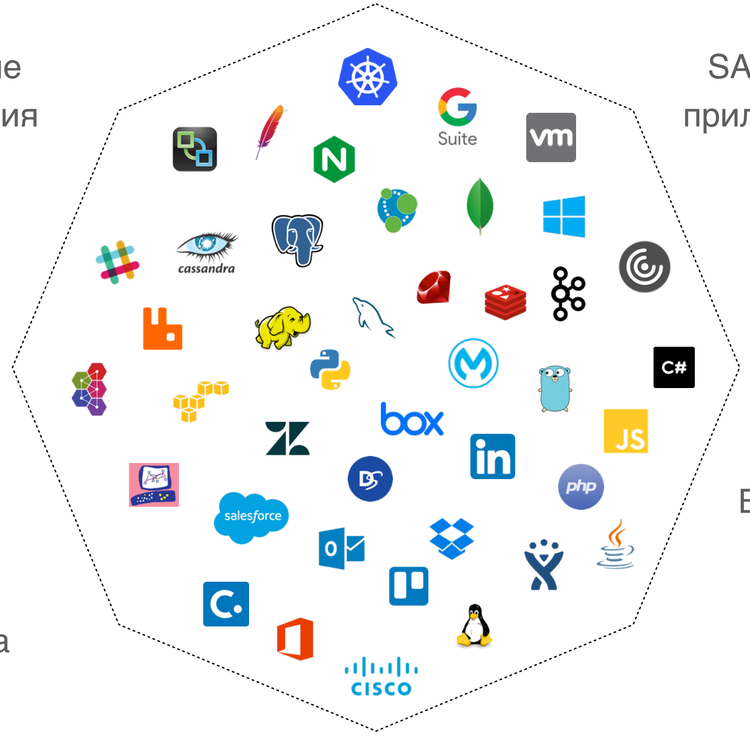
Технологический паззл

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 с простотой управлять всеми пользователями организации, выдавая доступы в зависимости от должности.

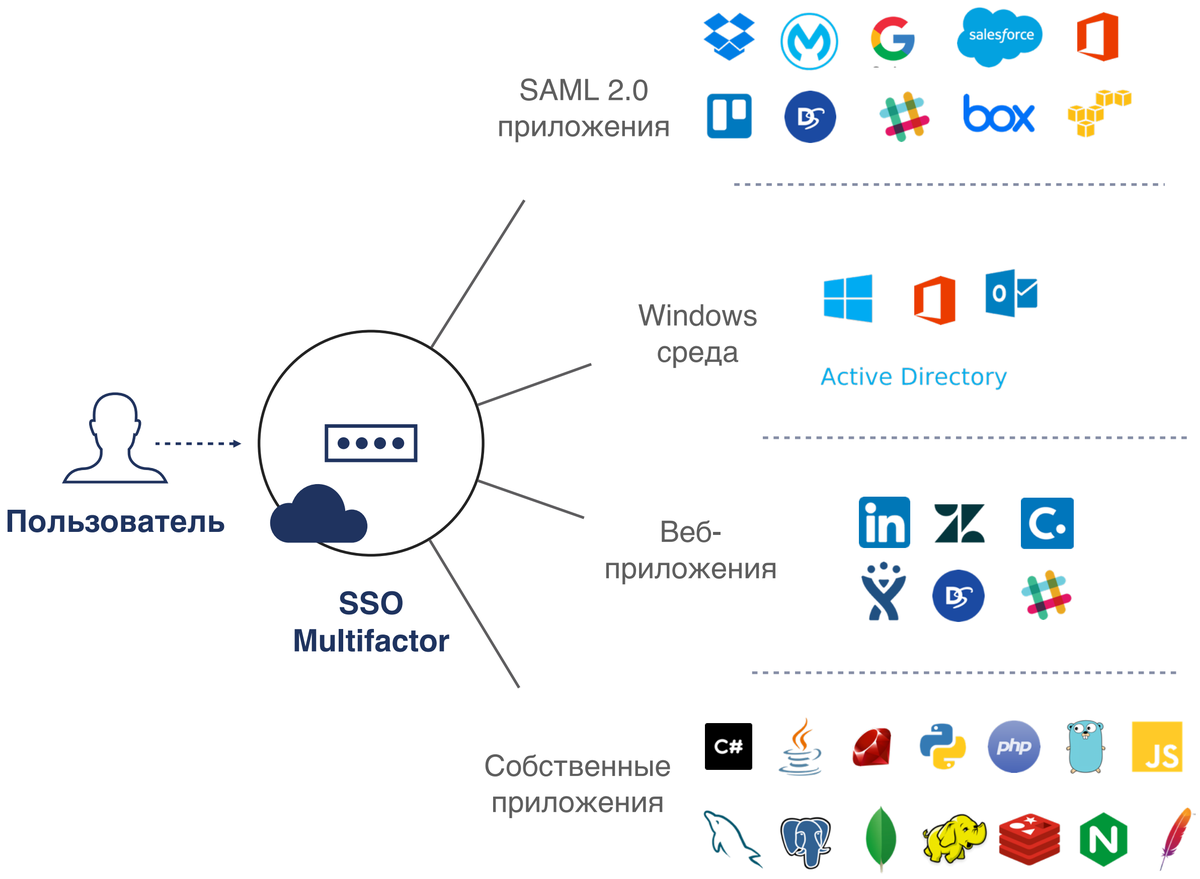
Улучшенный пользовательский опыт
Отпадает необходимость запоминать множество паролей и учётных записей. Возможность изменения паролей во всех сервисах в пару кликов.

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

Упрощённая связность
Интеграция нового приложения в инфраструктуру компании занимает меньше времени.



5. Регистрация 2FA пользователями

Подключение второго фактора доступа пользователями системы

3 режима настройки 2FA

1 Автоматическая регистрация

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Автоматическая регистрация SMS в качестве второго фактора доступа (синхронизация телефонных номеров с ActiveDirectory).

2 Регистрация в режиме самообслуживания

✓ 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.

✓ 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.

Пример 1: Регистрация 2FA в режиме диалога с пользователем

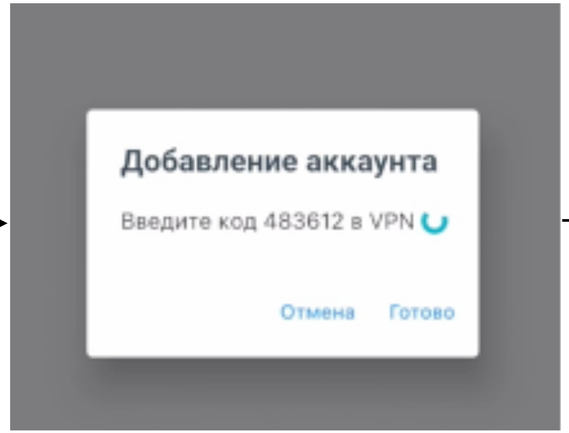
1 Выбор фактора

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 SMS обратно в клиент.

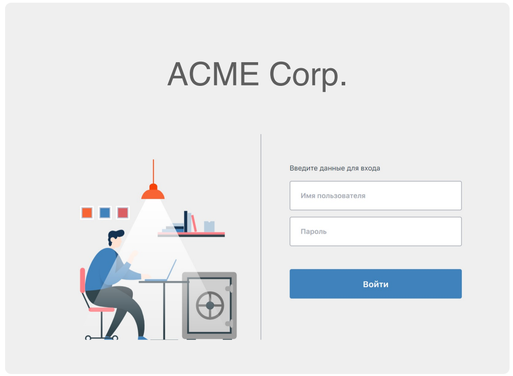
4 Готово!

Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

[1] Telegram, SMS, Приложение Мультифактор в случае защиты VPN и VDI соединений.

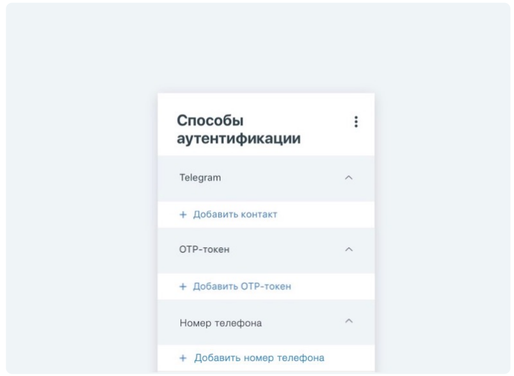
Пример 2: Регистрация 2FA на портале самообслуживания

1 Первое подключение



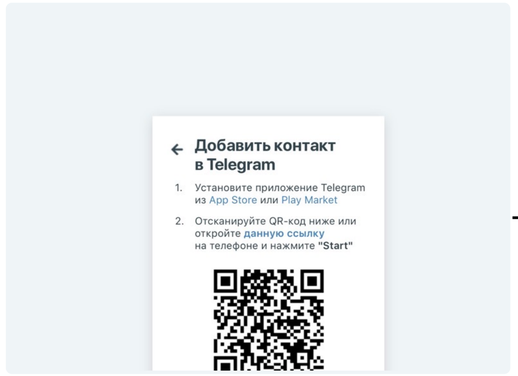
Пользователь проходит аутентификацию на Портале Самообслуживания (учетные данные Active Directory);

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, SMS, Звонок, Приложение Мультифактор 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?

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

Отказоустойчивость
Отказ облака MULTIFACTOR не скажется на работе вашего бизнеса. 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 и Яндекс.Облако 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 **99.98%**
- Техподдержка **7×24×1H**

[1] Горизонтальное масштабирование при необходимости

6. Нам доверяют

СОВКОМБАНК

positive technologies

НТВ ПЛЮС
ВСЕГДА. ВЕЗДЕ. НА ЛЮБОМ УСТРОЙСТВЕ

Ростелеком

СУЭК

QIWI БАНК

РОСАТОМ

S7 Airlines

РТЛабс
ГРУППА КОМПАНИЙ

FESCO

Major

м² метр квадратный

О'КЕЙ

МТС HOME

РЖД

HoReCa

- Реализована проверка второго фактора при входе в VPN;
- Срок внедрения MULTIFACTOR – 2 недели;
- Кол-во подключенных пользователей – более 1000;
- Inline enrollment - настройка второго фактора аутентификации в режиме интерактивного диалога с пользователем;
- Усиленная защита доступа к инфраструктуре компании.

С момента внедрения системы все сотрудники и подрядчики компании могут удаленно подключиться к корпоративной сети только с проверкой второго фактора.

Сервис также позволяет дополнительно отслеживать статистику и успешность подключений - такой встроенный функционал критически важен для обеспечения информационной безопасности компании.

Транспортно-логистическая отрасль

FESCO

- Реализована проверка второго фактора при входе в VPN;
- срок внедрения MULTIFACTOR – 1 месяц;
- проверка второго фактора аутентификации с помощью мобильного приложения Multifactor;
- легкий и интуитивно понятный онбординг пользователей при первом подключении с 2FA;
- усиленная защита доступа к инфраструктуре компании.

Major

- Реализована проверка второго фактора при входе:
  - в VPN;
  - веб-доступ к почте;
  - при подключении к удаленному рабочему столу;
  - при входе в CRM-систему.
- Кол-во подключенных пользователей – более 1000;
- Снижение нагрузки на ИТ-отдел заказчика за счет упрощенного онбординга пользователей.

ИТ-компании

positive technologies

- Все виды удаленных подключений к инфраструктуре компании защищены дополнительным фактором доступа;
- Реализован безопасный single sign-on (SSO, единый вход) в корпоративных приложениях.

РТЛабс®
ГРУППА КОМПАНИЙ

- Быстрая интеграция в ИТ-инфраструктуру заказчика;
- Интуитивный способ подключения пользователей;
- Подключение второго фактора аутентификации.

ИТ-компании

CloudPayments

- Реализована проверка второго фактора при входе в VPN;
- Срок внедрения MULTIFACTOR – 1 день!;
- Проверка второго фактора аутентификации с помощью мобильного приложения Multifactor;
- Усиленная защита доступа к ИТ-инфраструктуре компании.

Ростелеком Солар

- Реализована проверка второго фактора при входе в VPN;
- Срок внедрения MULTIFACTOR – 2 недели;
- Кол-во подключенных пользователей – 1900;
- Легкий и интуитивно понятный онбординг пользователей при первом подключении с 2FA;
- Снижение нагрузки с ИТ-отдела заказчика за счет функционала Inline enrollment.

Недвижимость

GloraX

- Защита VDI-подключений;
- Скорость внедрения – 1 месяц;
- снижение нагрузки на ИТ-отдел заказчика за счет функции Inline enrollment;
- Исключение риска несанкционированного доступа.

м² метр квадратный

- Защита подключений к межсетевым экранам и VPN-сервисам;
- Скорость внедрения – 3 недели;
- Кол-во подключенных пользователей – более 600;
- Защита ИТ-периметра компании.

Компанию представил
директор по продажам
Роман Коротун

r.korotun@multifactor.ru

Новости, инсайды
и идеи в наших соцсетях

/multifactor /multifactor_news