MULTIFACTOR

Просто. Надёжно. Безопасно.

Многофакторная аутентификация (MFA)
Единый вход (SSO)

1. Боли рынка

Проблемы удалённого доступа

Обзор

- **8 млн.** Человек в РФ работают дистанционно[1]
- **31%** Инцидентов ИБ связаны с угоном учётных записей[2]
- **20%** Рост числа внешних атак за полгода (ноя. 2020)[3]
- **65%** Компаний в РФ затрагивают растущие кибер-угрозы[1]

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.

$3.3 млн.

Средний ущерб от кибер-атак для компаний в РФ[4]

[1] По данным АО "Эр-Телеком Холдинг" и Gartner
[2] 2019 Verizon Data Breach Investigations Report
[3] По данным FBK Grant Thornton
[4] Доклад отдела борьбы с киберпреступностью Microsoft EMEA

Проблемы

1 Небезопасность удалённых подключений

- Вирусы, социальная инженерия, 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.

Реализация киберриска – вопрос времени, если превентивно не принять мер защиты подключений к корпоративным ресурсам.

2 Неэффективные процессы управления доступом

Высокая нагрузка на команду IT-поддержи в связи с онбордингом и оффбордингом пользователей, организацией удалённого доступа, обслуживанием учётных записей, смене забытых паролей и паролей с истёкшим сроком действия.

Результат простоя бизнес-процессов из-за нерешённых проблем с доступом – высокие финансовые и временные издержки.

2. Решение

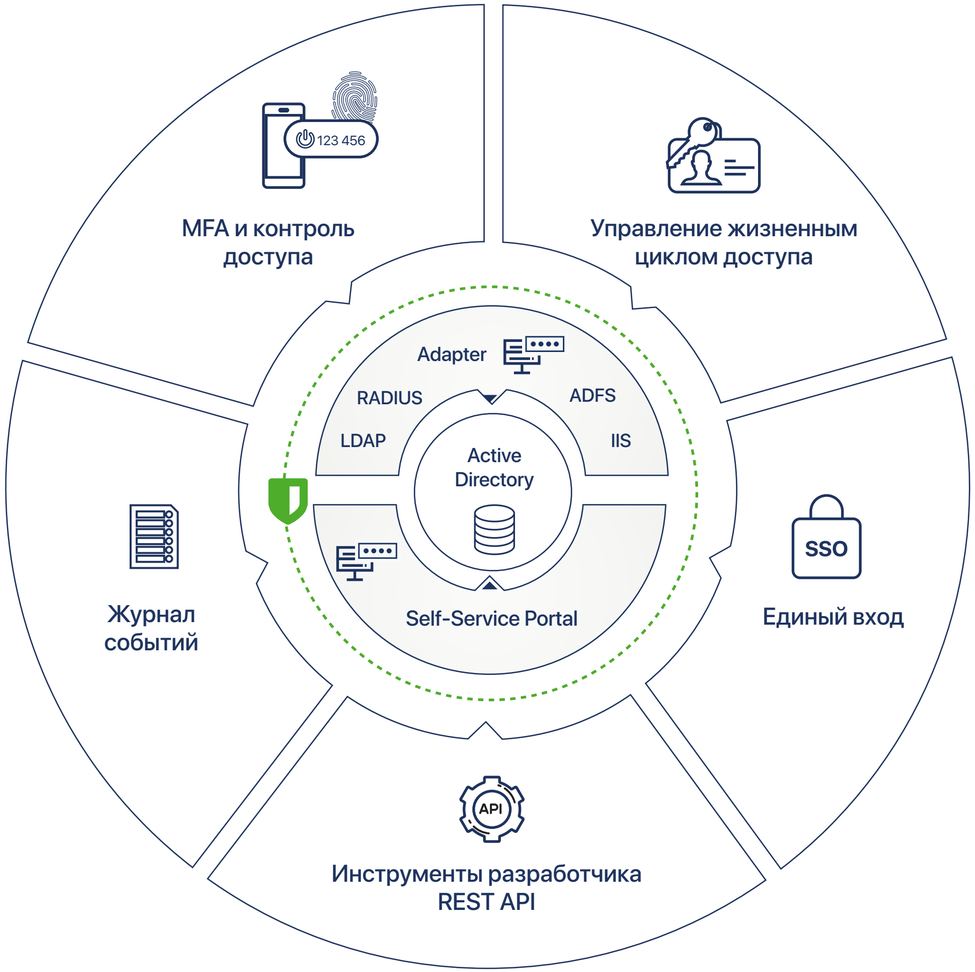
Продукт MULTIFACTOR

Мультифактор с одного взгляда

Сотрудники

Партнёры

Клиенты



1. **VPN**
   Check Point, 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

Решение MULTIFACTOR

Продукт в [реестре российского ПО]();

CAPEX
0₽

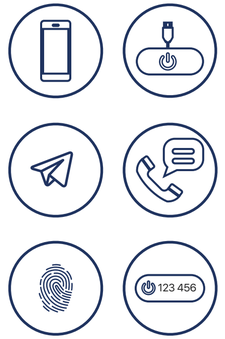
Не требует затрат на внедрение и инфраструктуру.

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.

Создаём 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 кибер-риском;
- Оптимизация резервов под кибер-риск;
- 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.

Почему MULTIFACTOR?

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

Отказоустойчивость
Отказ облака Мультифактор 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 датацентрах DataLine 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
Мультифактор 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

3. Обзор технологии

Многофакторная аутентификация (MFA)

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.

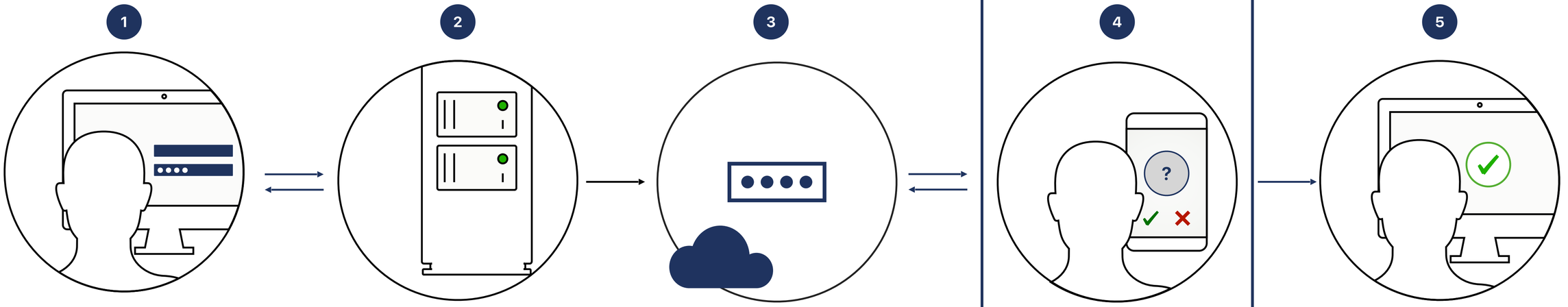
Поддерживаемые методы аутентификации

В таблице ниже представлены 6 основных методов проверки второго фактора, поддерживаемых Мультифактором, 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				✓	✓

MULTIFACTOR не получает доступ к вашим учётным данным

Система работает поверх основного метода аутентификации, и никогда не обрабатывает и не хранит пароли ваших пользователей.



1. Устройство пользователя

Проверка первого фактора

Пользователь самостоятельно вводит свой логин и пароль. Мультифактор не получает доступа к ним.

2. Внутренний периметр сети

Данные проверяются в вашей сети

Вы аутентифицируете пользователя с помощью Active Directory и отправляете запрос на 2FA аутентификацию в облако Мультифактор.

3.

Запрос отправлен в Мультифактор

Запрос на аутентификацию вторым фактором отправлен в облако Мультифактора, где реализована вся обработка.

4. Подтверждение доступа

Проверка второго фактора

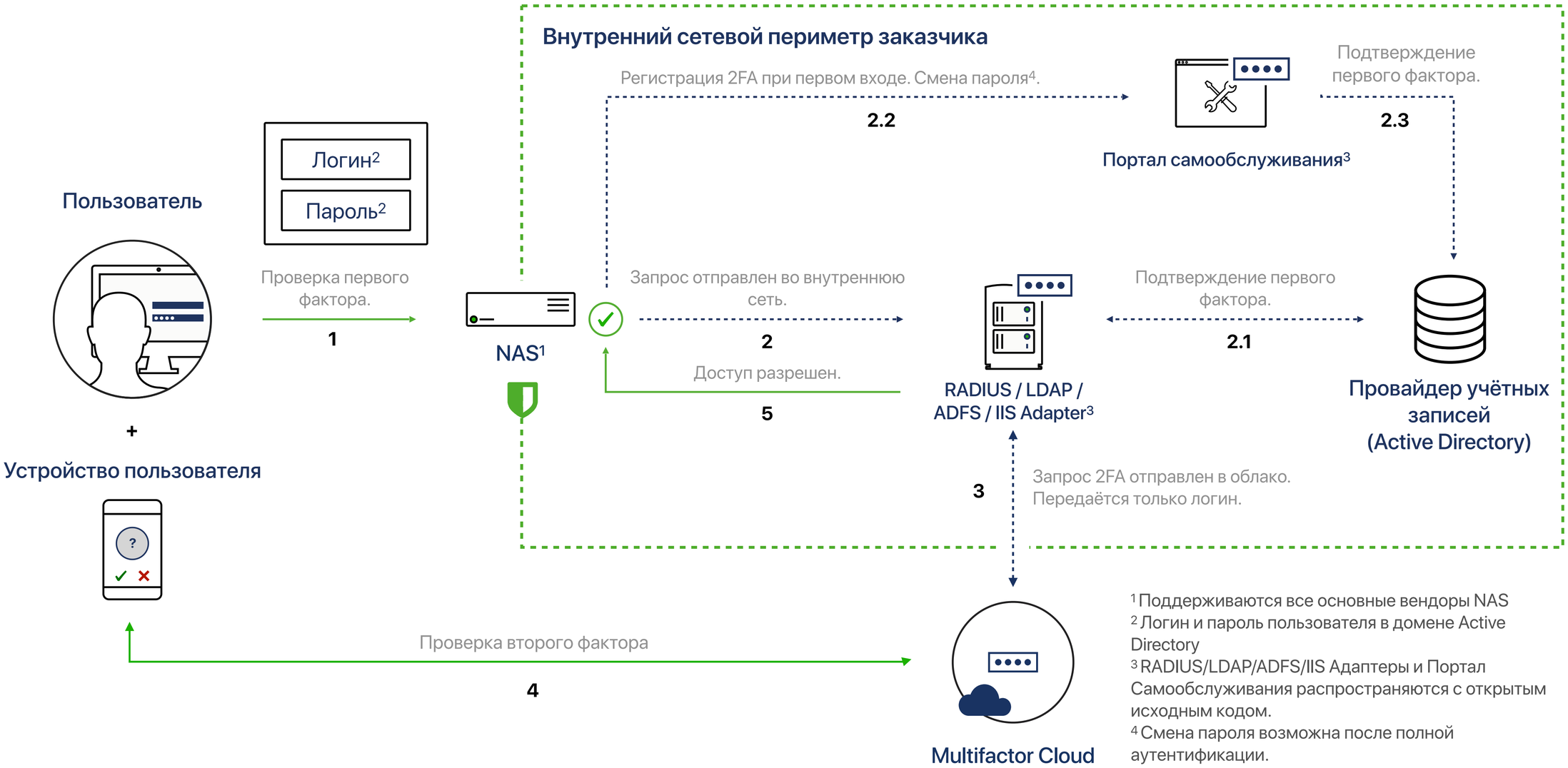
- Мобильное приложение Multifactor
- Telegram
- SMS или звонок
- OTP-токены

5. Устройство пользователя

Доступ разрешен

Пользователь залогинен в систему.

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.

Состав решения

1 Компоненты On-Premise

1. Портал самообслуживания

Расширение для Active Directory

- 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.

Мин. системные требования:
1 ядро CPU, 2Gb RAM, Windows Server 2012 и выше

2. RADIUS, LDAP, ADFS, IIS Адаптер

Адаптер для Active Directory

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

Мин. системные требования:
4 ядра CPU, 4Gb RAM, Windows Server 2012 и выше

2 Облако MULTIFACTOR

multifactor.ru

Безопасное размещение в ДЦ DataLine

- 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 **99.98%**

Техподдержка **7×24×1H**

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.

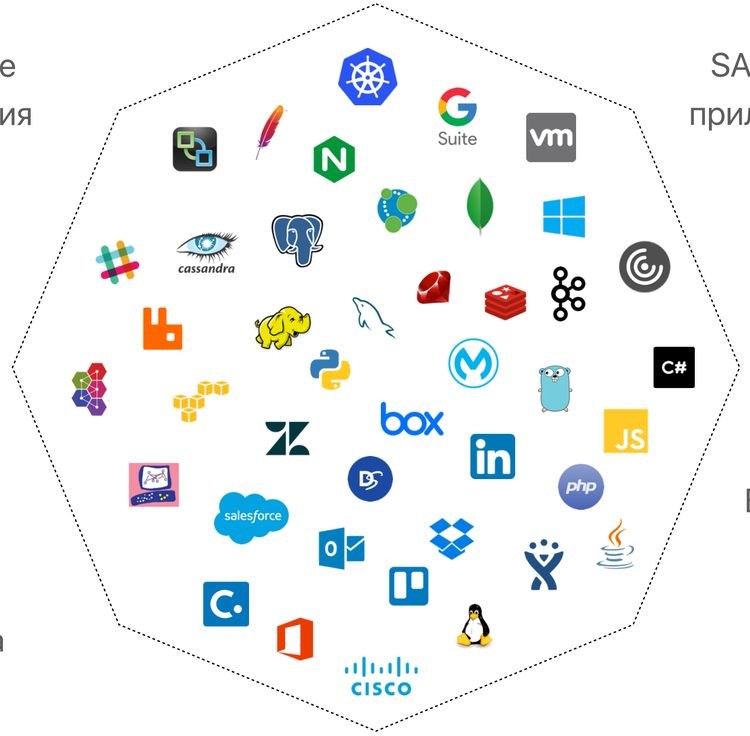
Технологический паззл

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.

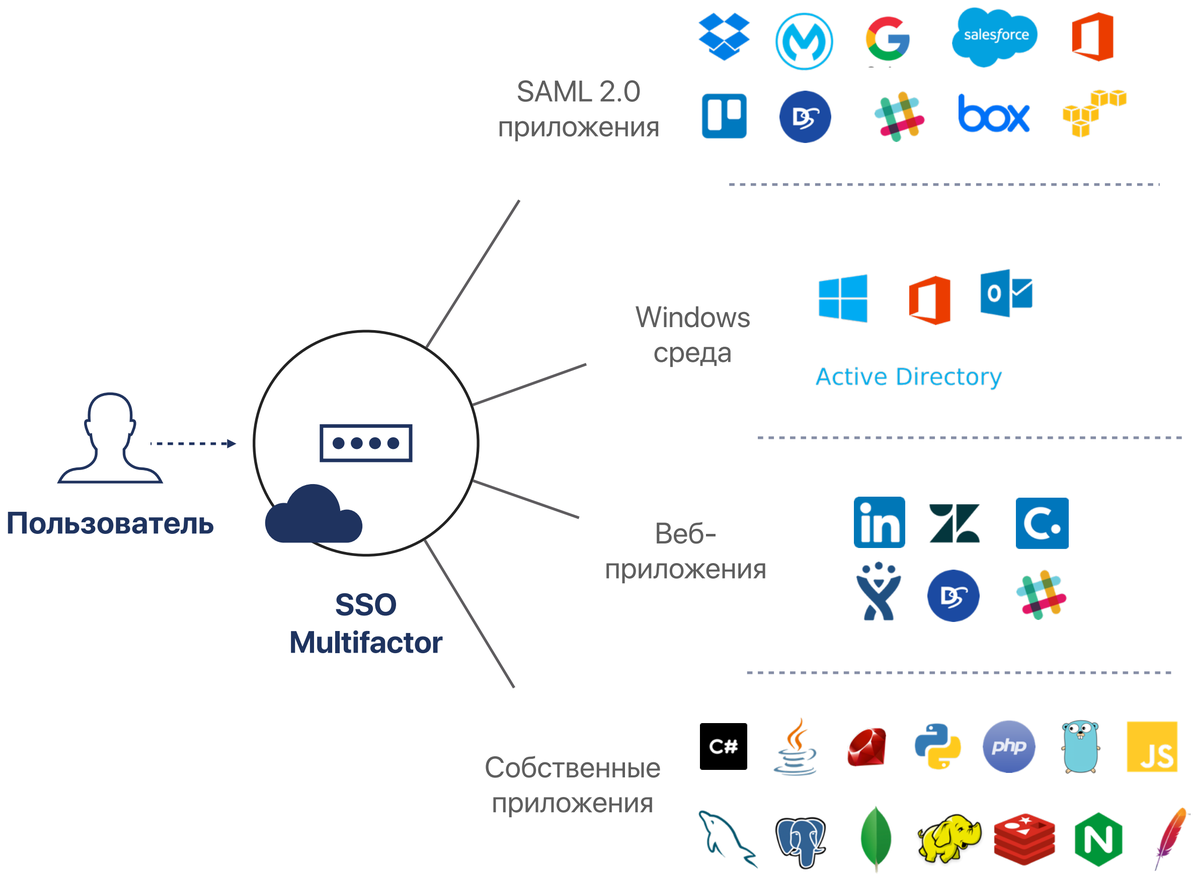
Улучшенный пользовательский опыт
Отпадает необходимость запоминать множество паролей и учётных записей. Возможность изменения паролей во всех сервисах в пару кликов.

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

✓ 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.

Пример 1: Регистрация 2FA в режиме диалога с пользователем

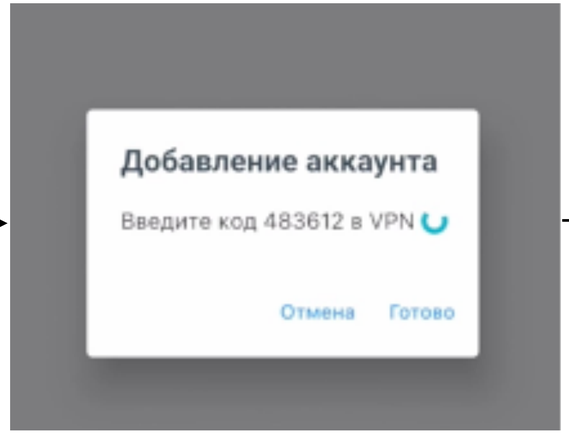
1 Выбор фактора

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.

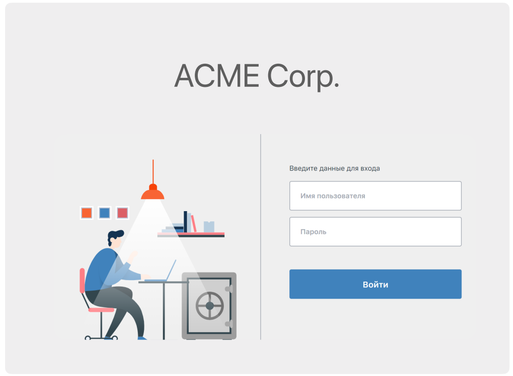
4 Готово!

Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

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

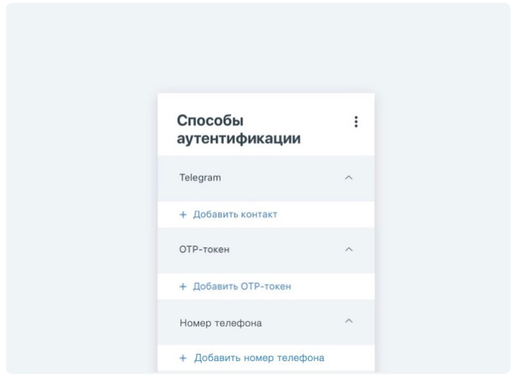
Пример 2: Регистрация 2FA на портале самообслуживания

1 Первое подключение



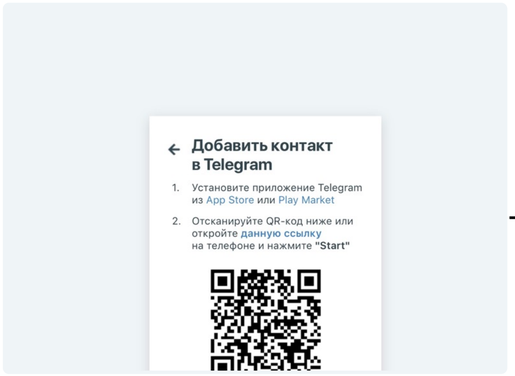
Пользователь проходит аутентификацию на Портале Самообслуживания (учетные данные Active Directory);

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.

7. О нас

Команда профессионалов

Миссия

Предоставляем разработчикам и бизнесу любого размера инструменты корпоративного класса для защиты своих информационных систем.

Компания

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

Реестр отечественного ПО

Решение MULTIFACTOR находится в реестре российского ПО.

Команда

Константин Ян CTO и CEO

Константин 14 лет занимается разработкой продуктов в сфере платежей и информационной безопасности. Со-основатель платежного сервиса CloudPayments – **exit Tinkoff**.

Виктор Чащин COO

Виктор – сертифицированный White Hat Hacker, с более чем 7 годами экспертизы в финтех безопасности.

Роман Башкатов CCO

Роман более 6 лет выстраивает эффективные коммерческие блоки в лидирующих IT бизнесах России.


control
option
command
A
S
D
F
Y
X
C
V
W
E
R