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 кибер-риска – 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 офбордингом 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 Мультифактор

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.

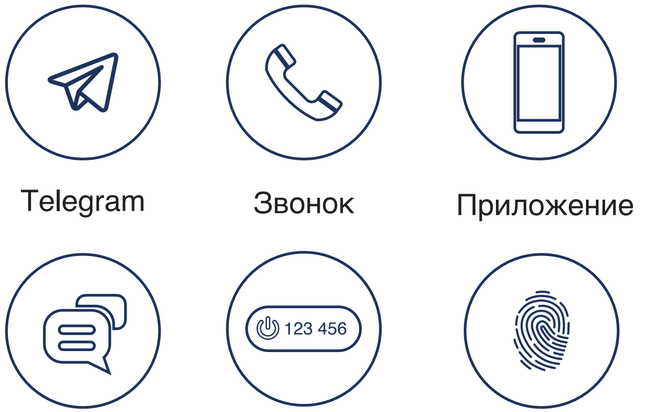
1 Первый фактор

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])

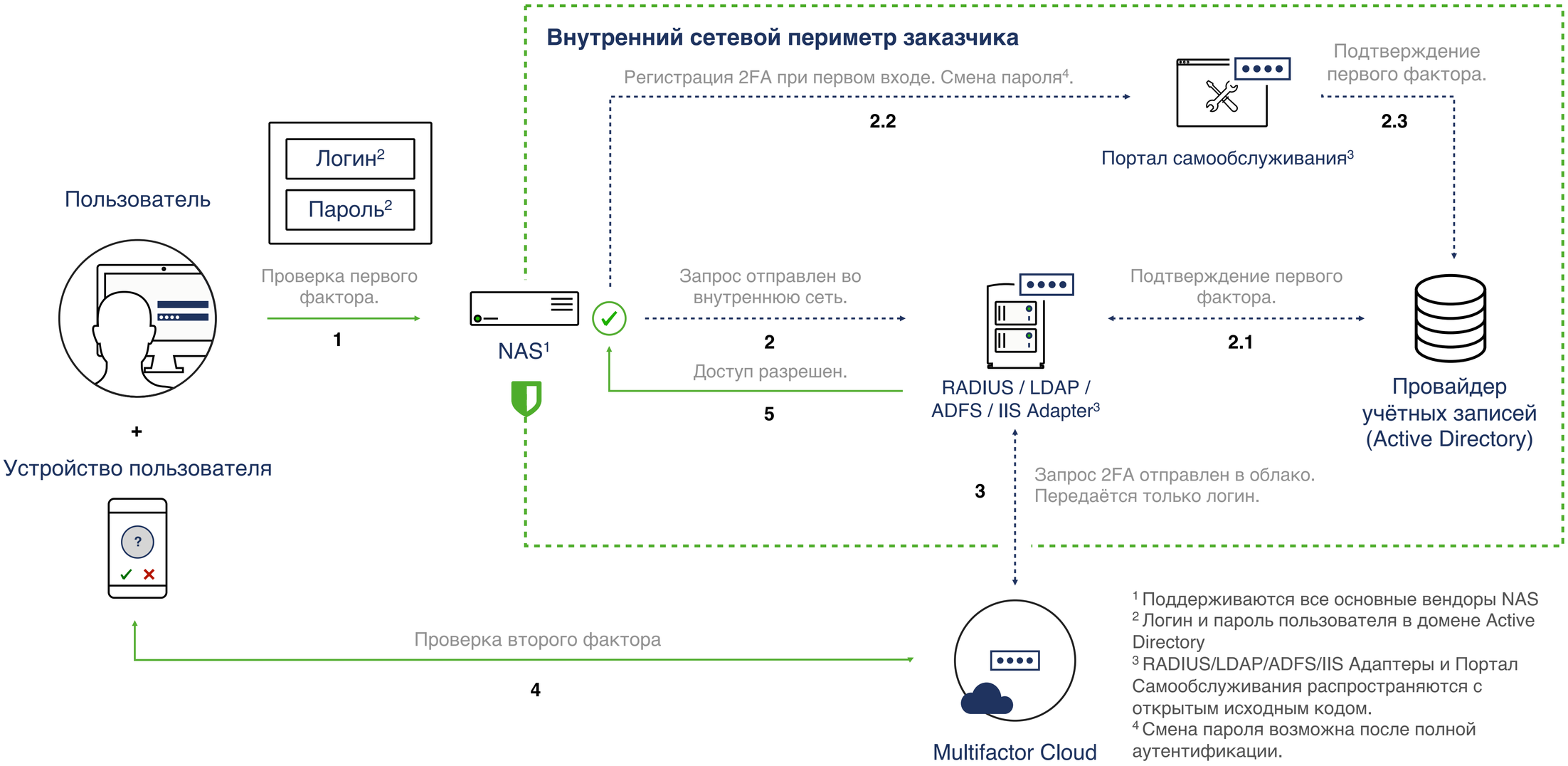
Биометрия[1]

3 Доступ

Доступ разрешён.

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

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.

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.

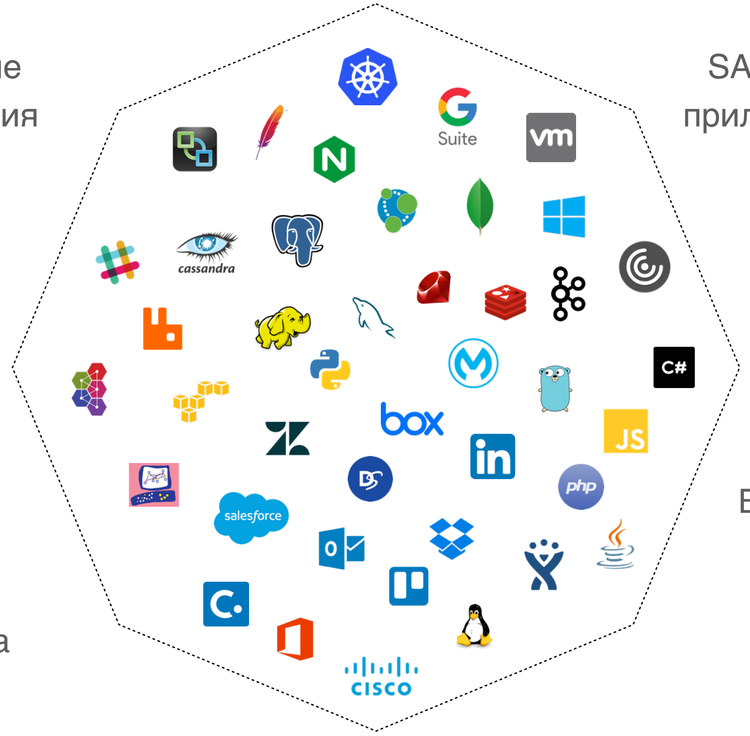
Технологический паззл

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 Мультифактор – 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.

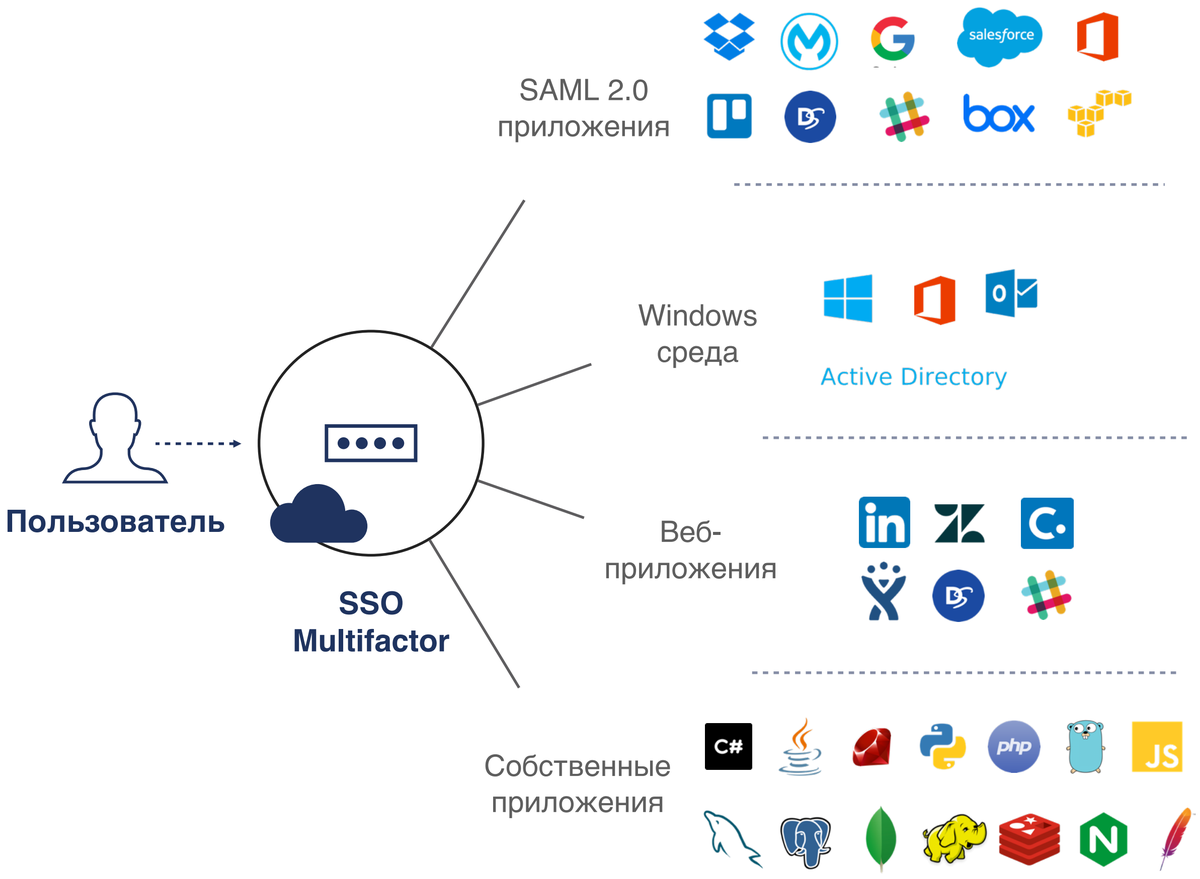
Улучшенный пользовательский опыт
Отпадает необходимость запоминать множество паролей и учётных записей. Возможность изменения паролей во всех сервисах в пару кликов.

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. 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 Мультифактор 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.

sales@multifactor.ru
+7 499 444 08 82