MULTI FACTOR

создано в МУЛЬТИ ФАКТОР

Система двухфакторной аутентификации и контроля доступа

МУЛЬТИ ФАКТОР

Создаём продукты для безопасной и стабильной работы ИТ-инфраструктуры бизнеса

5 лет
компании

4 продукта
в портфеле компании

200+
партнеров

PCI DSS
соответствует стандарту

ФСТЭК
лицензионный разработчик ФСТЭК

110+
интеграций с российскими разработками и платформами

1100+
успешных кейсов внедрения

В реестре отечественного ПО
продукты MULTIFACTOR, MULTIDIRECTORY

24/7
реагирование на инциденты

МУЛЬТИ ФАКТОР

Продукты компании

MULTI FACTOR

Система многофакторной аутентификации и контроля доступа для всех видов удалённого подключения

В реестре российского ПО № 7046

MULTI DIRECTORY

Российская служба каталогов MULTIDIRECTORY с ядром собственной разработки

В реестре российского ПО № 28333

MULTI PUSHED

Инструмент для отправки push-сообщений на любые устройства и ОС

MULTI STATUS

Распределённый облачный сервис анализа работы интернет-ресурсов

MULTI FACTOR

1100+ успешных кейсов внедрения

Вкусно — и точка

ВТБ

РЖД

DNS

CloudPayments

Алроса

Positive Technologies

Сбер Лизинг

Солар

Demetra Holding

Invitro

СУЭК

Россети

Альфа Страхование

HeadHunter

Трансмаш Холдинг

Спортмастер

MANGO OFFICE

MULTI FACTOR

Киберугрозы для бизнеса в России — новая реальность

Резкий рост киберугроз

Россия входит в ТОП-8 самых атакуемых стран в 2024 году [1]

Масштабные утечки данных

37% успешных кибератак на российские компании в 2024 году начинались с компрометации учётных данных сотрудников [2]

Уязвимости подрядчиков

— угроза для всех (13% от всех кибератак в 2024 году) [3]

Ужесточение требований регуляторов

Последствия

- Прямой и косвенный финансовый ущерб
- Снижение доверия со стороны заказчиков и партнёров
- Кража интеллектуальной собственности и раскрытие коммерческой тайны
- Штрафы от регуляторов

[1] По количеству DDOS-атак согласно данным компании StormWall
[2] По данным центра исследования киберугроз Solar 4RAYS
[3] По данным “Лаборатории Касперского”

MULTI FACTOR

Чем больше компания, тем дороже обойдётся инцидент

Финансовые издержки

Приостановление деятельности (из расчёта 5 дней)	Сорванные сделки	Восстановление инфраструктуры и расследование	Инвестиции в усиление безопасности
2,5 млн. ₽	**до 5 млн. ₽**	**3–5 млн. ₽**	**3–5 млн. ₽**

Убытки до 17,5 млн. ₽ за инцидент

Отток клиентов	Выкуп	Штрафы регуляторов
5% клиентской базы для B2B-компаний, 10-20% — для B2C	5-10% от годовой выручки компании	до 500 млн. ₽

Правовые последствия для должностных лиц

Штраф за нарушение №405-ФЗ

От 400 000 до 800 000 ₽

Расходы могут достигать:

- для малого бизнеса — 40 млн.
- для среднего — до 110 млн.
- для крупного — до 425 млн. (без учёта штрафов)[1]

+ расходы на судебные разбирательства, падение стоимости акций, дополнительные расходы на PR и маркетинг

[1] "Оценка ущерба от утечек информации и затрат на ликвидацию последствий", аналитический отчет Infowatch

MULTI FACTOR

Простое и надёжное решение для двухфакторной аутентификации

MULTIFACTOR — это российская система двухфакторной аутентификации и контроля доступа для Linux- и Windows-серверов, систем виртуализации и облаков, серверов Exchange, точек доступа VPN, VDI, корпоративных приложений и сайтов

Решение в реестре российского ПО № 7046

Простая интеграция

Поддерживает все основные протоколы доступа (RADIUS, LDAP, OAuth 2.0, OpenID Connect)

и службы каталогов (MULTIDIRECTORY, Active Directory, OpenLDAP, FreeIPA и др.)

0 рублей на инфраструктуру

Без затрат на приобретение, обслуживание серверов и на лицензии сторонних вендоров

Быстрый старт

Ввод в эксплуатацию от 2 часов, техподдержка пилотных проектов

Защищает любые типы ресурсов

Windows-инфраструктура:

Windows Logon, Outlook Web Access (OWA), Windows VPN, NPS, и др.

Linux-инфраструктура:

OpenVPN, SSH, Sudo и др.

Межсетевые экраны:

Cisco, UserGate, CheckPoint, Mikrotik, С-Терра и др.

Системы виртуализации:

VMware vCloud, HUAWEI Cloud и др.

Remote Desktop Gateway:

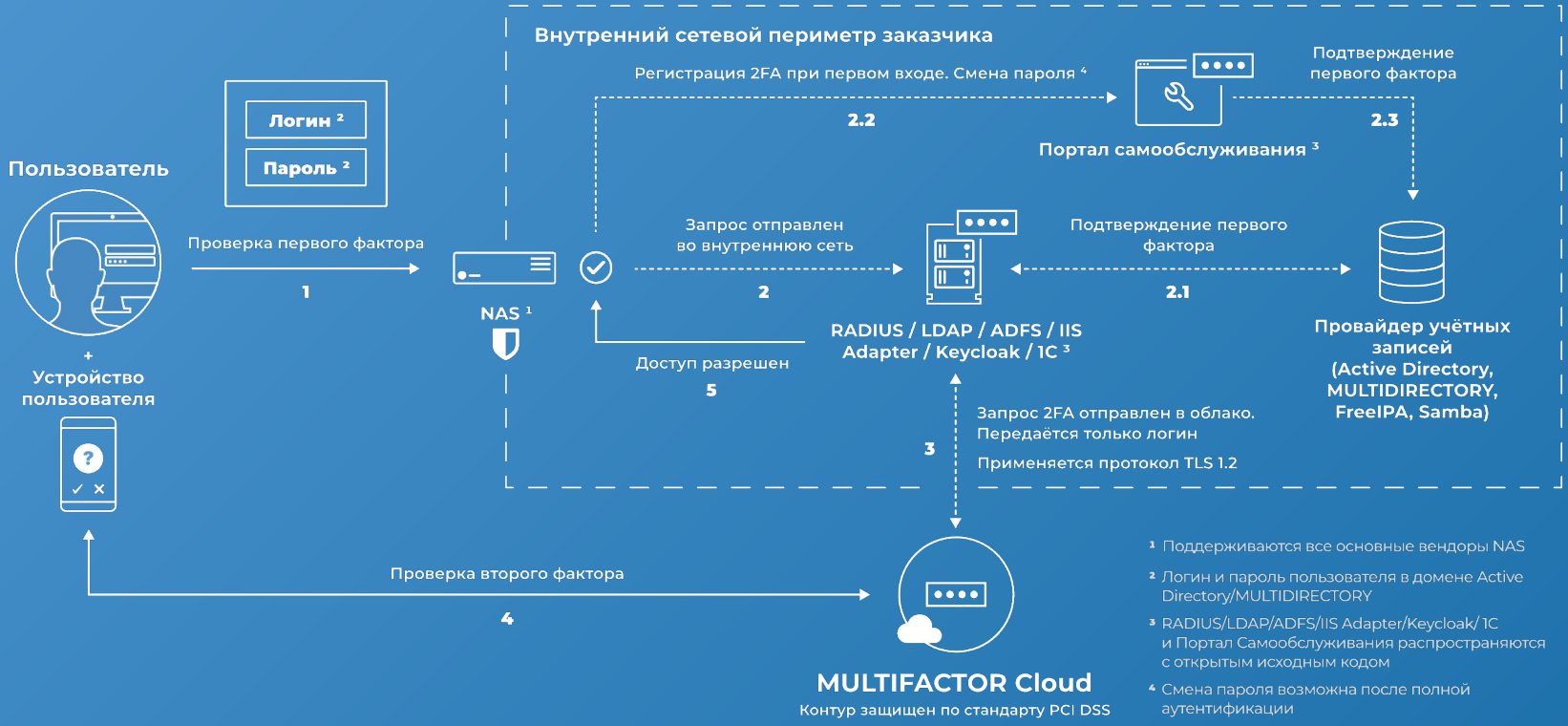
Citrix, RD Gateway, VMware Horizon и др.

Точки доступа Wi-Fi

Различные приложения:

Zabbix, Ansible AWX, 1С-Битрикс24, HRBOX, Redmine, МТС Линк, Пассворк, СКДПУ Айти Бастион и др.

Высокоуровневая схема решения



1 Поддерживаются все основные вендоры NAS

2 Логин и пароль пользователя в домене Active Directory/MULTIDIRECTORY

3 RADIUS/LDAP/ADFS/IIS Adapter/Keycloak/ 1C и Портал Самообслуживания распространяются с открытым исходным кодом

4 Смена пароля возможна после полной аутентификации

MULTI FACTOR

MULTIFACTOR — гибридное решение, которое берёт лучшее от облачных и локальных систем

Сочетает гибкость и масштабируемость облака с уровнем контроля и соответствием нормативам безопасности, которые одобряет служба ИБ

SLA 99,99%

Облачная часть

- MFA и контроль доступа, управление жизненным циклом доступа
- Единый вход SSO — для удобного и безопасного входа во все сервисы заказчика
- Личный кабинет администратора и журнал событий
- API и инструменты разработчика — для интеграции с проприетарными приложениями и серверной инфраструктурой

Linux Windows

Компоненты On-Premise

- LDAP / RADIUS / ADFS / IIS Adapter / Keycloak / 1C
- Портал самообслуживания SSP позволяет пользователям решать проблемы с доступом без участия ИТ-поддержки

Все методы аутентификации в одном решении

MULTIFACTOR поддерживает привычные пользователям сценарии входа и предлагает редкие, недоступные конкурентам варианты:

	VPN И VDI	LINUX-ИНФРАСТРУКТУРА	WINDOWS-ИНФРАСТРУКТУРА	ОБЛАЧНЫЕ ПРИЛОЖЕНИЯ	API (WEB)
ПРИЛОЖЕНИЕ MULTIFACTOR собственная разработка	✓	✓	✓	✓	✓
TELEGRAM редкая функция на рынке	✓	✓	✓	✓	✓
СМС ИЛИ ЗВОНОК	✓	✓	✓	✓	✓
OTP-ТОКЕНЫ (АППАРАТНЫЕ И ПРОГРАММНЫЕ)	✓	✓	✓	✓	✓
U2F-/FIDO-ТОКЕНЫ				✓	✓
БИОМЕТРИЯ				✓	✓

MULTI FACTOR

Три режима настройки 2FA под разные масштабы и требования

1. Автоматическая регистрация

удобно · быстро · средняя сложность интеграции

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

2. Регистрация в режиме самообслуживания

удобно · быстро · простая интеграция

Диалог с пользователем

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

удобно · средняя скорость подключения · средняя сложность интеграции

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

3. Регистрация вручную

достаточно удобно · медленно · простая интеграция

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

2FA в вашем мобильном приложении

Без онбординга сотрудников и настройки методов аутентификации — пользователи автоматически подключаются к 2FA при входе в ваше приложение

Сценарии использования

- Бесшовный онбординг по API. Нет необходимости устанавливать отдельное приложение
- Стандартный сценарий с самостоятельной регистрацией по QR

Кому подходит

Для компаний с собственным мобильным приложением и системами, для которых требуется 2FA-защита

Инструкция по настройке здесь →

MULTI FACTOR

Продвинутые возможности MULTIFACTOR

Push-уведомления

Через собственный сервер (инструмент MULTIPUSHED)

Directory Sync

Сервис для ОС Windows, который помогает автоматически синхронизировать пользователей из Active Directory

Защита от перебора

Паролей и сессионных атак — CAPTCHA, блокировка учётной записи, блокировка IP-адреса источника

SSP (портал самообслуживания)

Позволяет пользователю самостоятельно настраивать и подтверждать владение вторым фактором и изменять пароль после полной аутентификации. Поддерживает Exchange ActiveSync

Режим ByPass

Позволяет группам или отдельным пользователям входить без второго фактора

Защита второго фактора перед первым

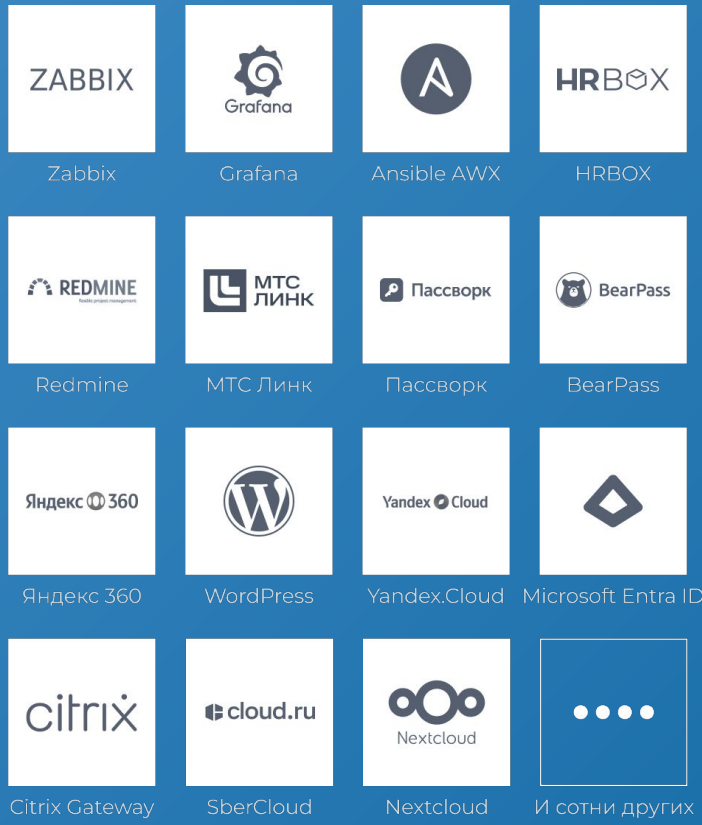
Сначала подтверждается второй фактор (push-уведомление, сообщение в Telegram, OTP-код и другие), а затем — первый (логин и пароль)

MULTI FACTOR

Единый вход Single Sign-On (SSO)

SSO позволяет сотруднику получить доступ ко всем интегрированным сервисам с одним набором учётных данных

Повторный ввод данных (логин/пароль, push, Telegram, биометрия, СМС-код и т.д.) не требуется



MULTI FACTOR

Преимущества SSO

Максимум удобства

Одна аутентификация для всех корпоративных систем

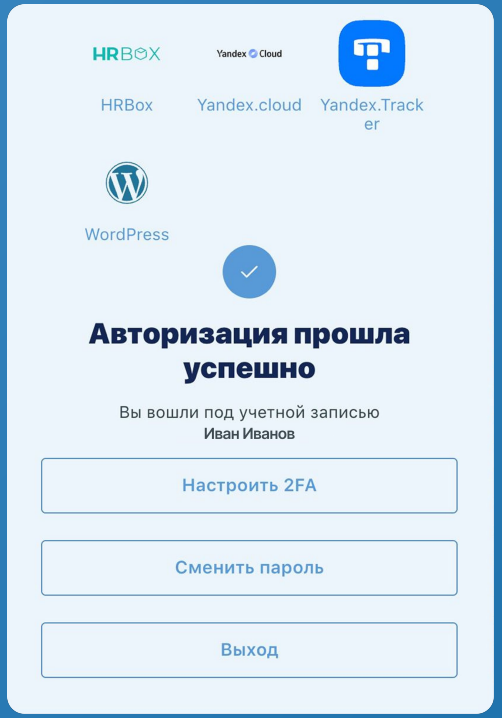
Снижение нагрузки на ИТ-отдел

Быстрый онбординг с первого дня и офбординг сотрудников «без дыр», минимум запросов на сброс паролей

Защита учётных данных

Централизованное управление доступом, исключаются слабые и повторяющиеся пароли

Российская альтернатива Keycloak и ADFS



MULTI FACTOR

MULTIFACTOR — это:

Безопасность

Система не обрабатывает и не хранит пароли пользователей, а все учётные, персональные и сессионные данные передаются только в зашифрованном виде

Масштабируемость

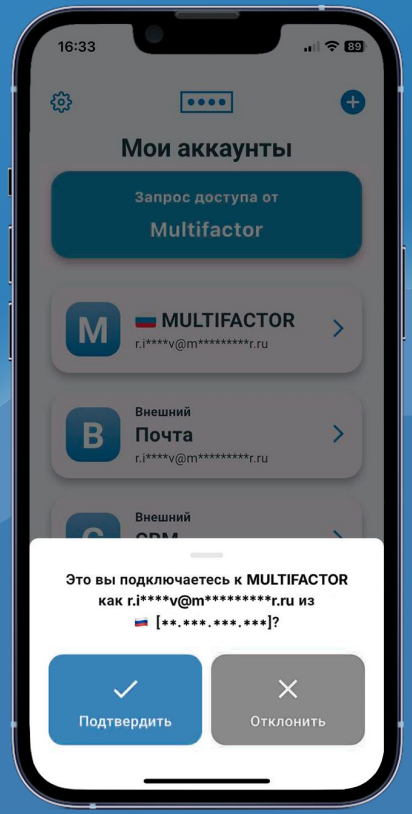
Нет ограничений по количеству пользователей и ресурсов, можно добавить любую бизнес-логику и различные интеграции

Удобство

Множество вариантов аутентификации, единый вход SSO и портал самообслуживания пользователей

Отказоустойчивость

Облако MULTIFACTOR обеспечивает SLA 99,99% и размещено в дата-центрах DataLine, Selectel и LinxCloud с многоуровневой физической защитой, резервными интернет-каналами и источниками питания, а также защитой от DDoS



Контакты

Остались вопросы?

Давайте обсудим, как MULTIFACTOR может работать именно в вашей компании

sales@multifactor.ru

multifactor.ru

+7 499 444 08 82

ВКОНТАКТЕ ДЗЕН TenChat

Наш Телеграм-канал

MULTI FACTOR

СОЗДАНО В МУЛЬТИ ФАКТОР