



БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ ЗДЕСЬ



multifactor.ru



Наша миссия

Создаём экосистему продуктов для безопасности ИТ-инфраструктуры бизнеса.



200+ партнеров



1100+ успешных кейсов внедрения



50+ интеграций с российскими разработками и платформами



710 000 + пользователей системы (по итогам 2024 г.)



Команда опытных профессионалов



Кастомизация решения под бизнес-цели заказчика



Реагирование на инциденты **24/7**



Соответствие стандарту **PCI DSS версии 4.0**

Реестр отечественного ПО

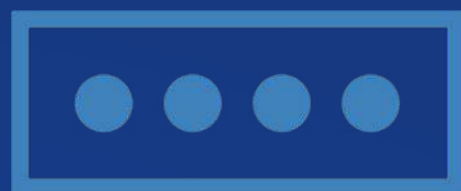
Решение MULTIFACTOR находится в реестре российского ПО [№7046](#).

Решение доступно бесплатно до трех пользователей

[Подключить](#)



MULTIFACTOR: продукты



MULTIFACTOR

Флагманский продукт компании — система многофакторной аутентификации и контроля доступа для всех видов удалённого подключения MULTIFACTOR

Решение включено в реестр
российского ПО
под номером 7046



MultiDirectory

Российская служба каталогов MultiDirectory с открытым исходным кодом и бесплатной Community-версией

PUSHED

PUSHED

Сервис push-уведомлений PUSHED для отправки и автоматизации push-сообщений на любые платформы



Нам доверяют



Вкусно и точка



ВТБ



РЖД



DNS



CloudPayments



Алроса



Positive Technologies



Сбер Лизинг



Солар



Demetra Holding



Invitro



СУЭК



Альфа
Страхование



Россети



HeadHunter



Трансмаш
холдинг



Спортмастер



Росводоканал



Боли рынка

01





₽ 100 МЛН

Максимальные оценки ущерба от утечек информации в российских организациях ¹

1 млрд

Количество утекших записей персональных данных в России за I полугодие 2024 г. ²

2,38 млн записей ПДн

В ходе одного инцидента в среднем утекает в России ²

99% утечек

Носят умышленный характер ²

На 10%

Выросло количество утечек в России за первое полугодие 2024 г. ²

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 InfoWatch «[Оценка ущерба от утечек информации и затрат на ликвидацию последствий](#)»

² По данным аналитического отчета InfoWatch: «[Утечки информации в мире и России за первое полугодие 2024 года](#)»



Штрафы за утечки ПДн

₽ 3-5 млн

Для компаний, если утечка затронула от 1000 до 10 000 субъектов персональных данных и/или от 10 000 до 100 000 уникальных идентификаторов пользователей.

₽ 5-10 млн

Суд может назначить компаниям при утечке данных 10 тыс. – 100 тыс. субъектов или 100 тыс. – 1 млн идентификаторов.



Проблемы

01 Боли рынка



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.

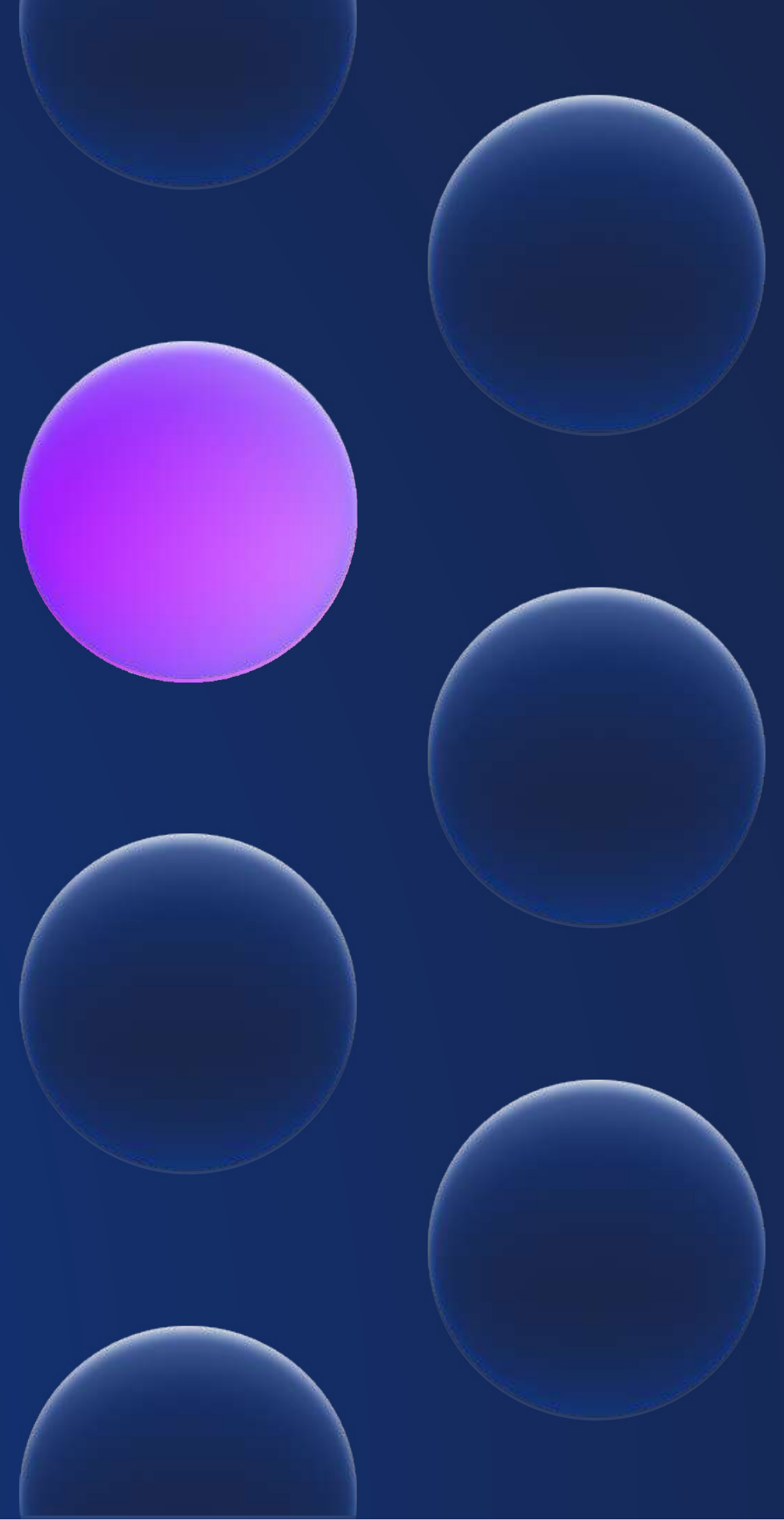


Реализация киберриска — вопрос времени, если превентивно не принять мер защиты подключения к корпоративным ресурсам.



Решение

02





MULTIFACTOR

Сотрудники

Партнёры

Клиенты



Провайдер учётных записей

- [MultiDirectory](#) – служба каталогов от МУЛЬТИФАКТОР
- Active Directory
- Linux Astra Directory
- NPS
- Samba 4
- Freeipa

✓ Защита входа

✓ Простая интеграция

✓ Покрытие всей инфраструктуры



Отечественные и зарубежные VPN-шлюзы

- [UserGate](#)
- [С-Терра](#)
- [КриптоПро NGate](#)
- [Континент 4](#)
- [Ideco UTM](#)
- Рубикон
- [CheckPoint](#)
- [Cisco](#)
- [FortiGate](#)
- [Mikrotik](#)
- [OpenVPN](#)



Облачные приложения, виртуализация, web

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



Linux

- [SSH](#)
- [SUDO](#)
- [OpenVPN](#)
- PAM
- и др.



VDI

- [VMware Horizon](#)
- [Citrix](#)
- [Remote Desktop](#)
- и др.



Windows

- [Windows Logon](#)
- [VPN](#)
- [RD Gateway](#)
- [NPS](#)
- и др.



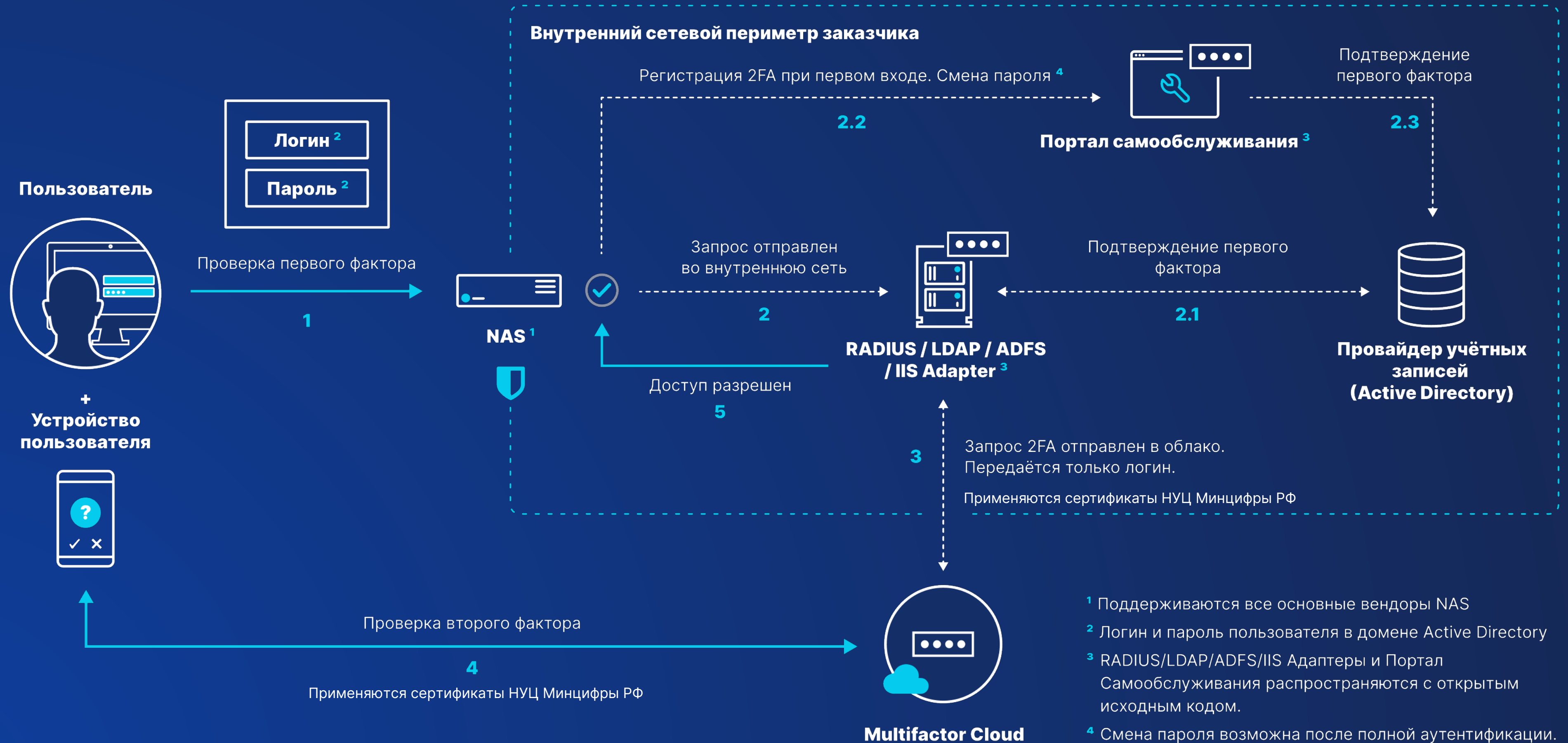
Другое ПО

- [СКДПУ АйТи-Бастион](#)
- [1С-Bitrix24](#)
- [Точки доступа Wi-Fi](#)
- все Desktop-приложения



SIEM-системы

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

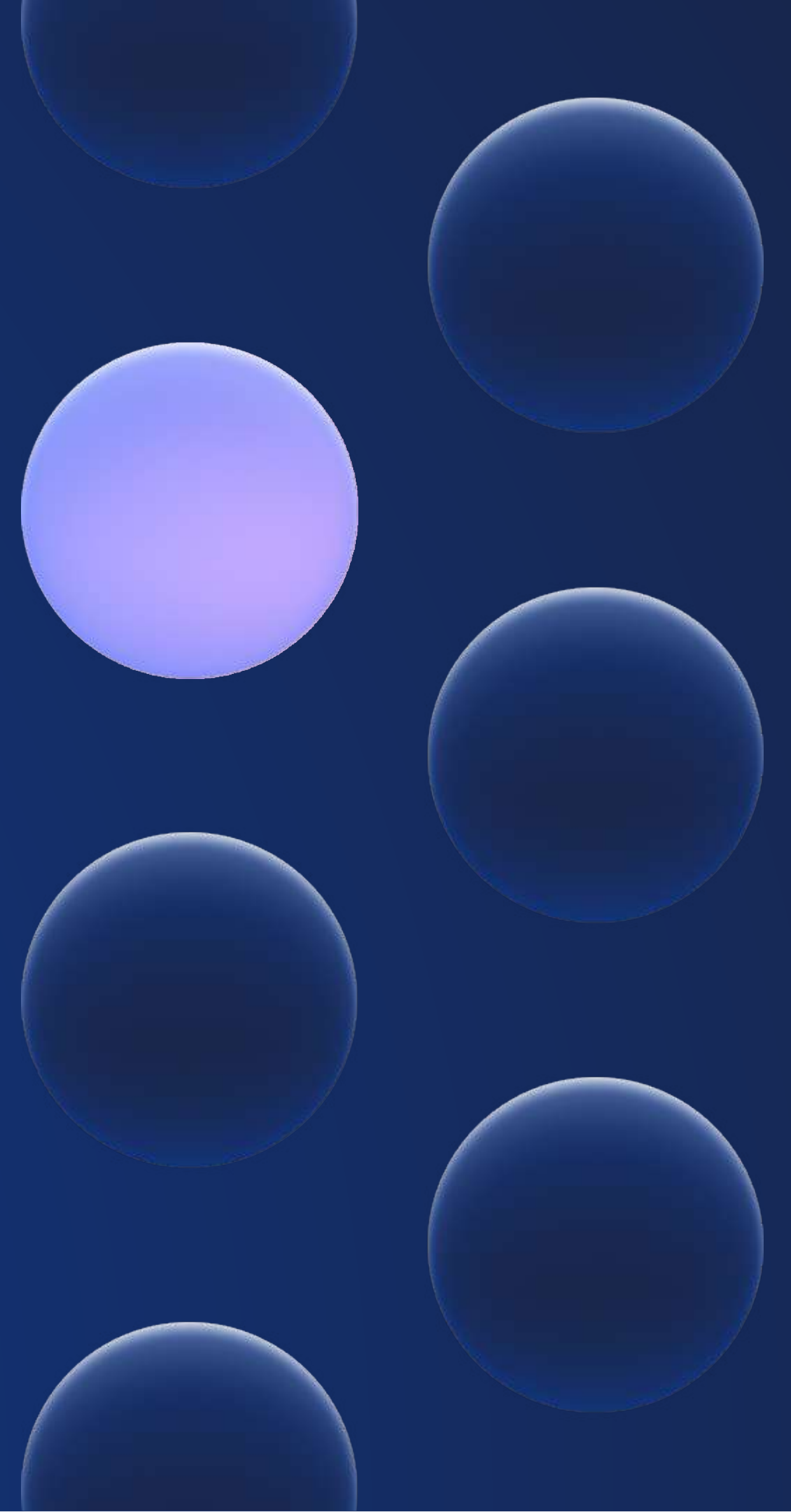


- ¹ Поддерживаются все основные вендоры NAS
- ² Логин и пароль пользователя в домене Active Directory
- ³ RADIUS/LDAP/ADFS/IIS Адаптеры и Портал Самообслуживания распространяются с открытым исходным кодом.
- ⁴ Смена пароля возможна после полной аутентификации.



Обзор технологии MFA

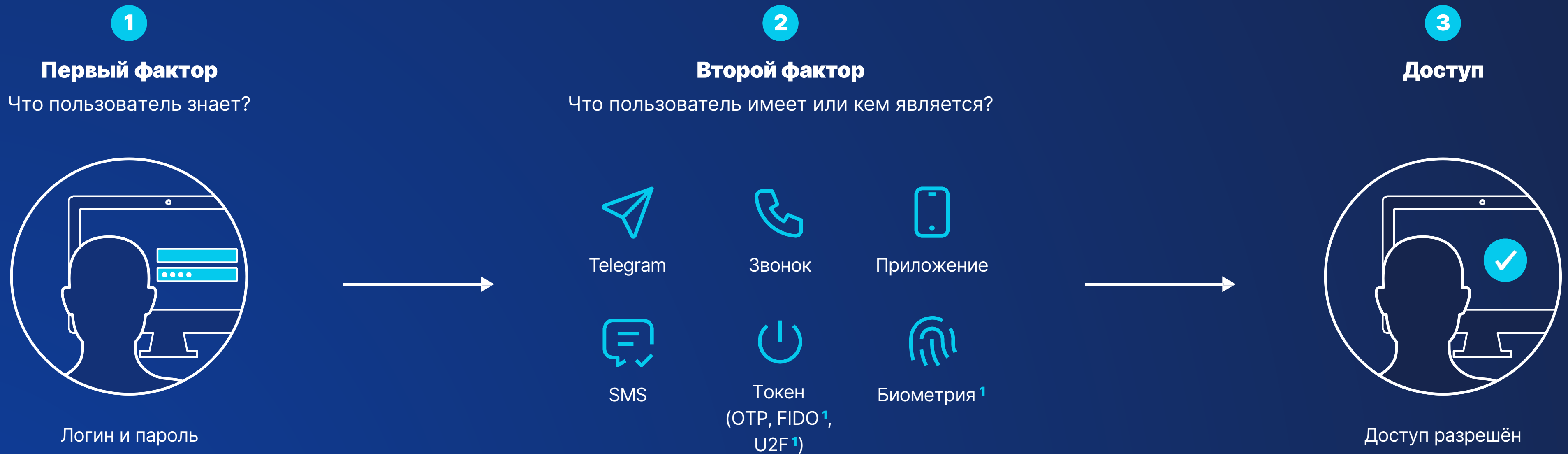
03





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.









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



Поддерживаемые методы аутентификации

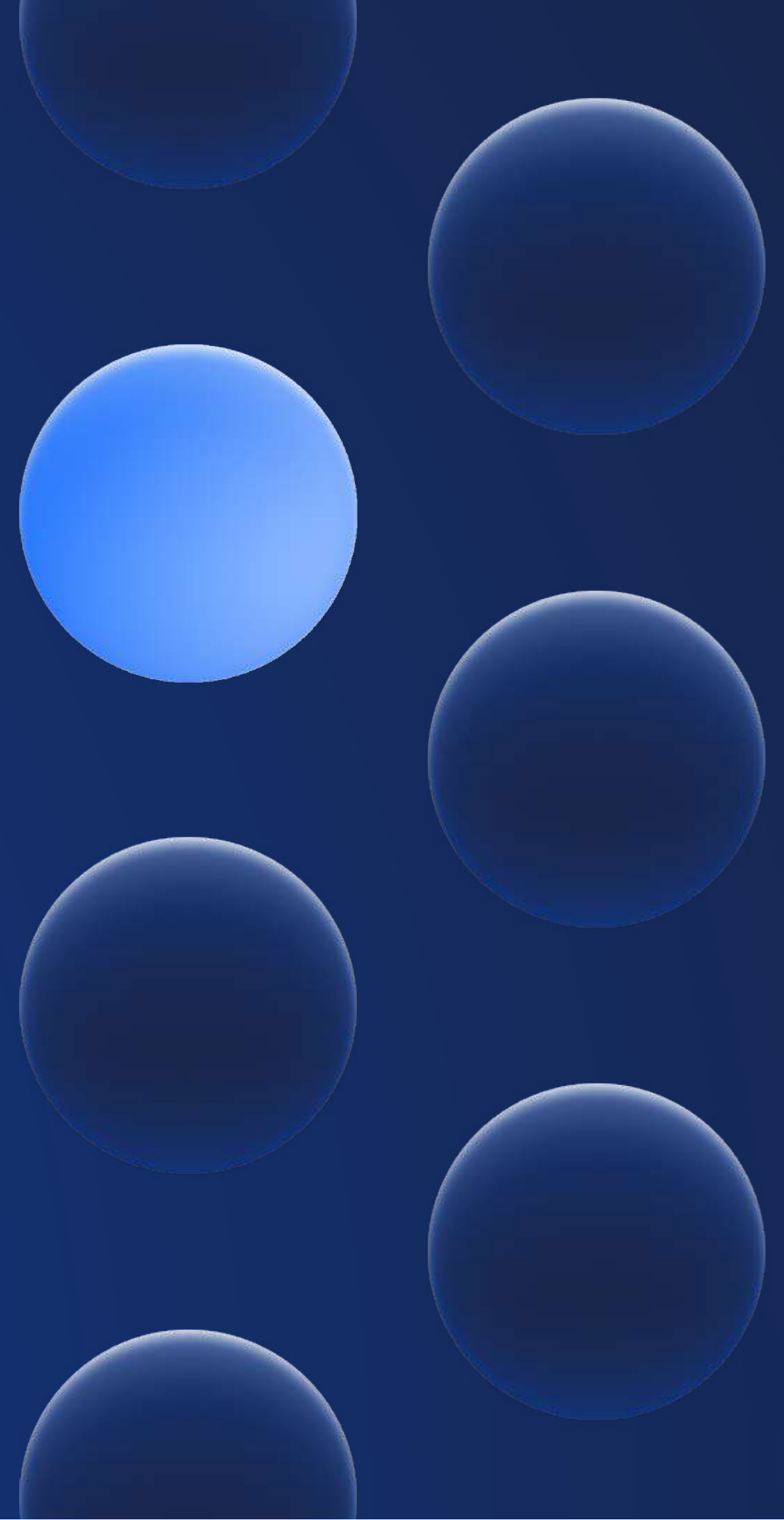
В таблице представлены 6 основных методов проверки второго фактора, поддерживаемых MULTIFACTOR, в зависимости от сценария использования.

	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)

04





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

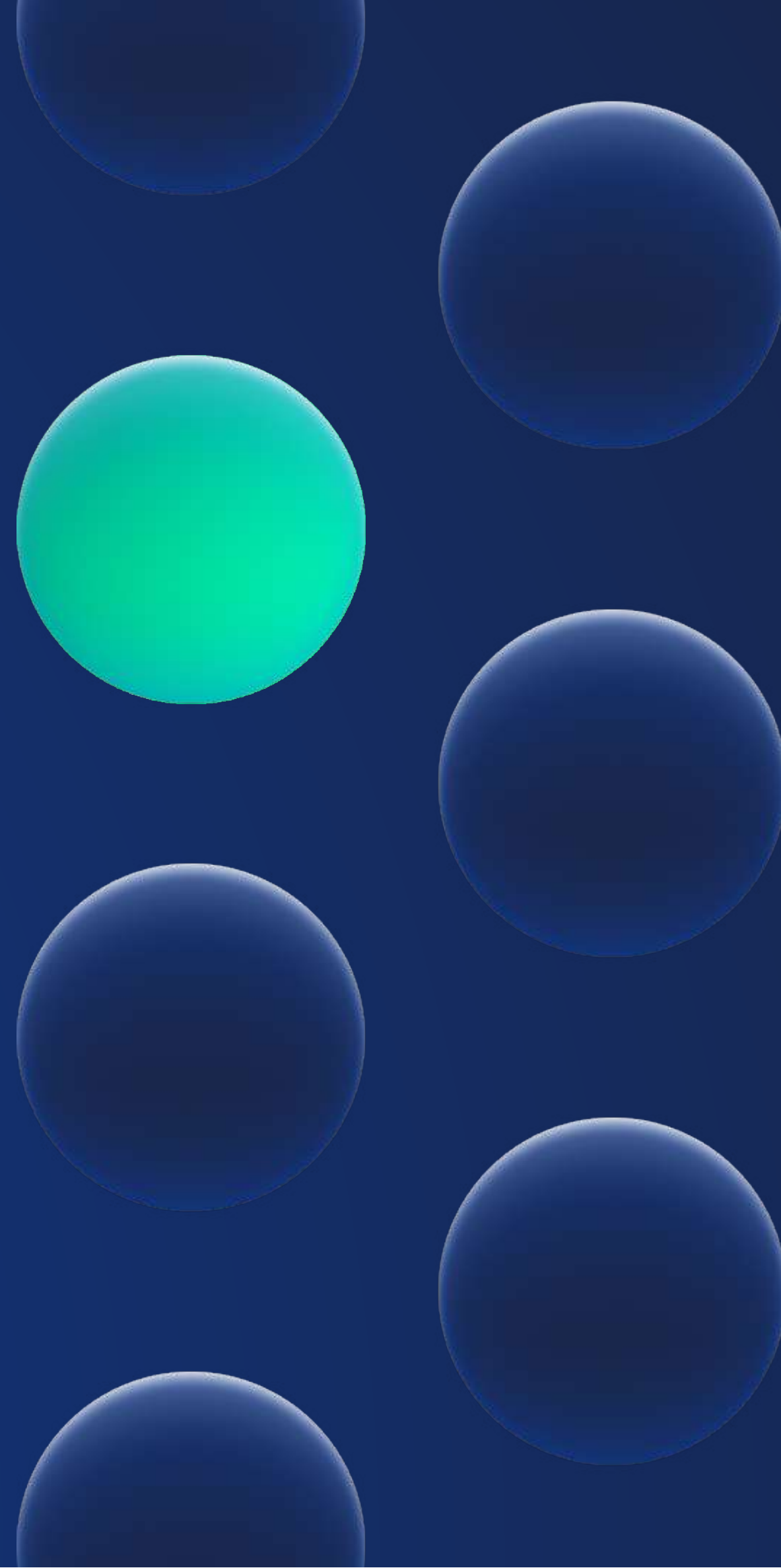
2Gb RAM

Windows Server 2012 и выше



Обзор технологии Единый вход (SSO)

05





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.



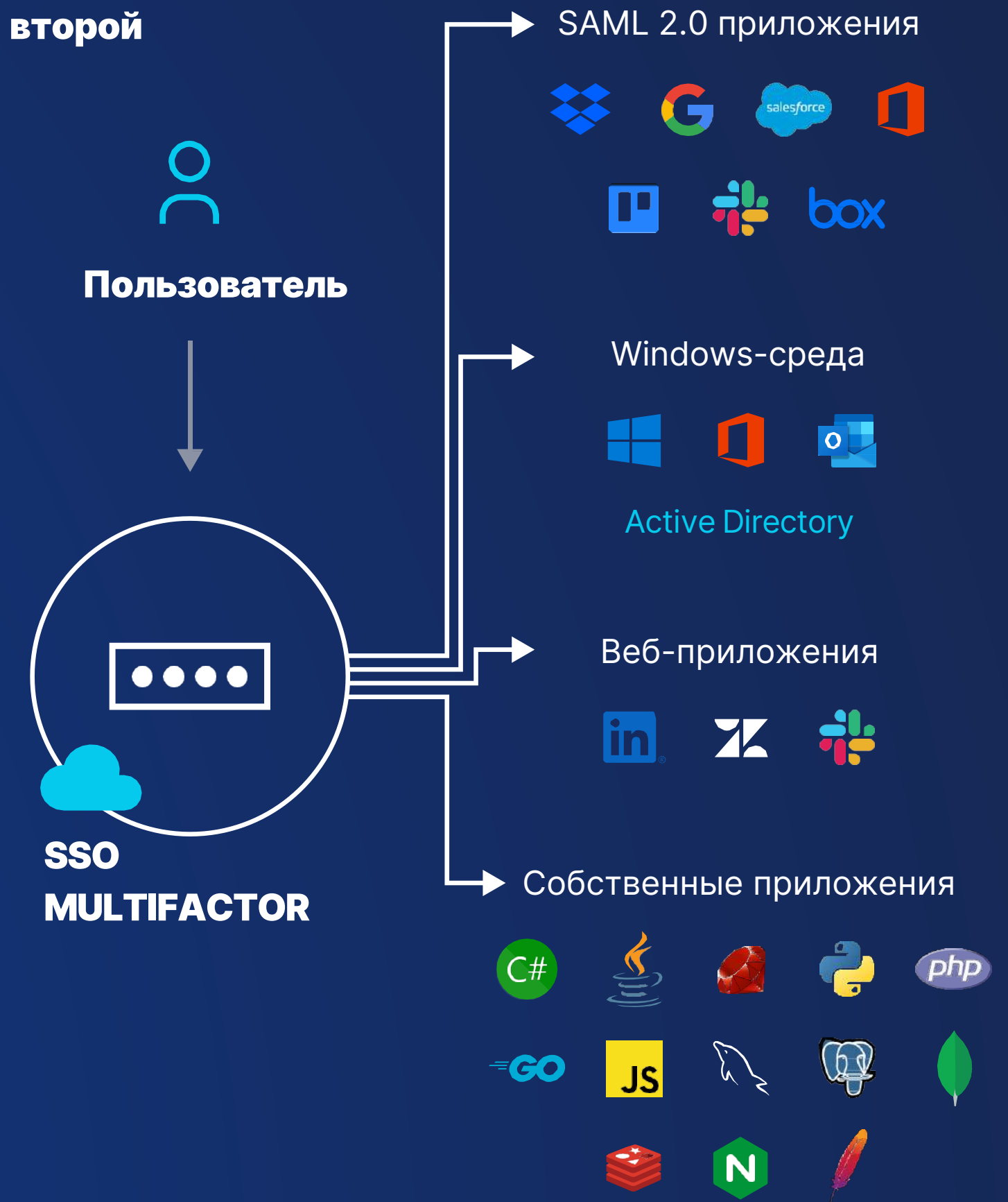
Увеличенная продуктивность

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



Упрощённая связность

Интеграция нового приложения в инфраструктуру компании занимает меньше времени.





Состав решения

06





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 LinxCloud

- 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

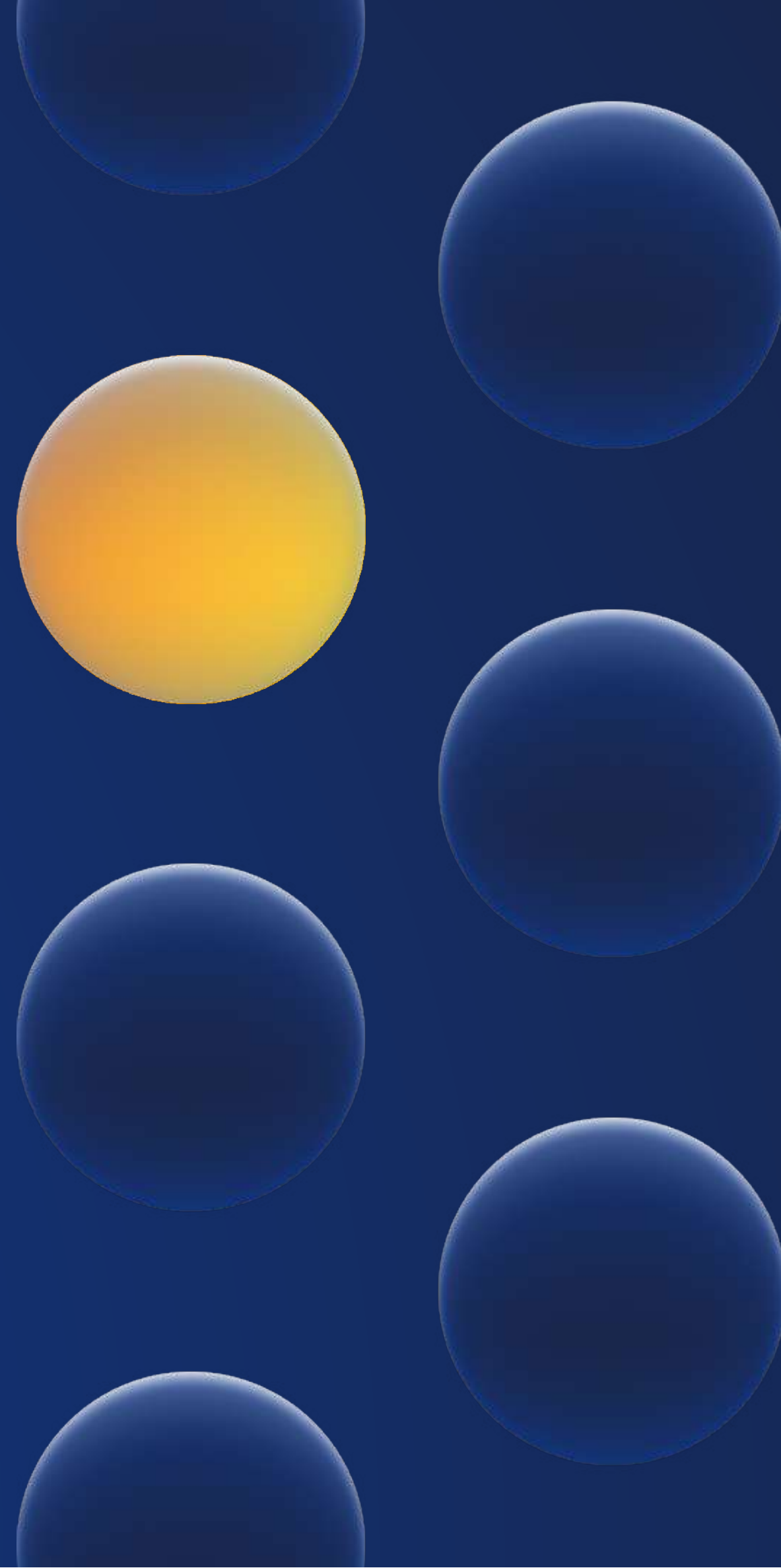
● Аптайм **99.99%**

● Тех. поддержка



Почему MULTIFACTOR?

07





Высокая доступность

Аптайм 99.99% 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, Linx 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



MULTIFACTOR



Остались вопросы?

sales@multifactor.ru

+7 499 444 08 82

multifactor.ru

Наши соц.сети



[@multifactor](https://vk.com/multifactor)



[/multifactor](https://t.me/multifactor)

[Мы в TenChat](#)



[@multifactor_news](https://t.me/multifactor_news)



[@multifactor9508](https://www.youtube.com/multifactor9508)