Avanpost MFA+

Система многофакторной аутентификации для широкого спектра корпоративных систем с поддержкой стандартных протоколов в on-premise

- быть свободным
- быть легким на подъем
- быть уверенным

Ведущий разработчик систем аутентификации и управления доступом

Продуктовая линейка решений аутентификации

AVANPOST

AVANPOST FAM
Federated Access Manager (On-prem)

Федеративное управление идентификацией

Современный адаптивный центр управления многофакторной аутентификацией в корпоративных приложениях с поддержкой мультидоменных инфраструктур и федерации удостоверений.

AVANPOST MFA+
Multi-factor Authentication Plus (On-prem)

Многофакторная аутентификация

Провайдер многофакторной аутентификации с поддержкой всех современных методов аутентификации, гибкой настройкой факторов через удобный интерфейс администратора.

+ дополнительные опции

AVANPOST Cloud Identity
Cloud Multi-factor Authentication (Cloud)

Облачная многофакторная аутентификация

Облачный провайдер многофакторной аутентификации для корпоративных систем с поддержкой стандартных протоколов.

В разработке

AVANPOST ESSO
Single Sign-on (On-prem)

Единая точка входа для корпоративных приложений

Единая точка защищенной аутентификации для корпоративных систем без поддержки стандартных протоколов.

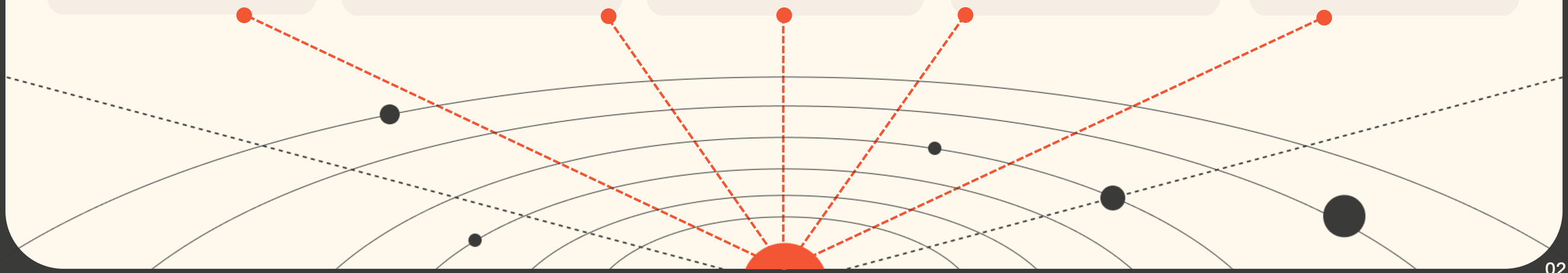
В разработке

AVANPOST Web SSO
Identity Management

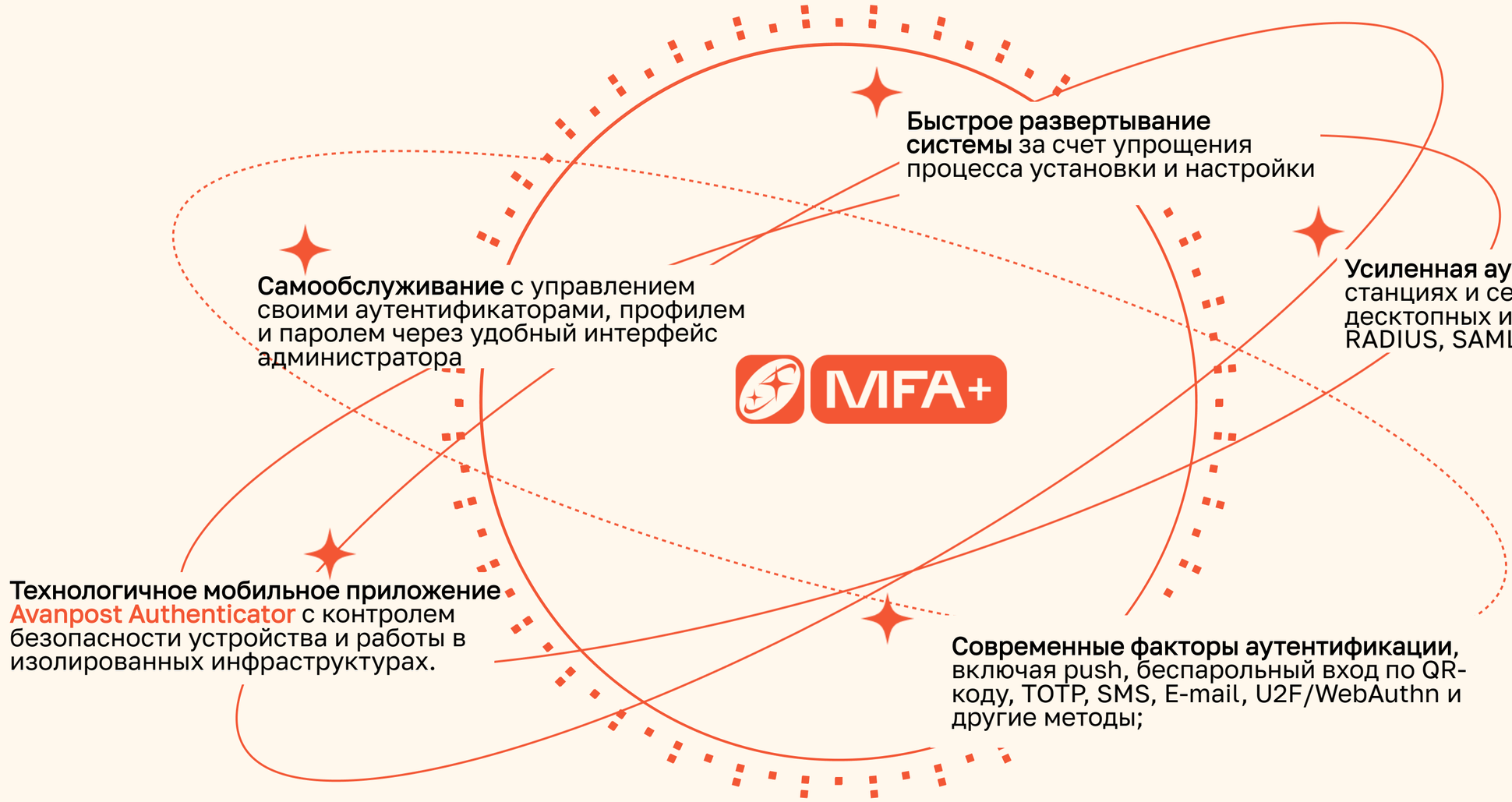
Единая точка входа для web приложений и API

Единая точка входа для веб-приложений, технологичных сервисов и API.

+ дополнительные опции



Конкурентные преимущества Avanpost MFA+



Быстрое развертывание системы за счет упрощения процесса установки и настройки

Самообслуживание с управлением своими аутентификаторами, профилем и паролем через удобный интерфейс администратора

Усиленная аутентификация в рабочих станциях и серверах, VPN, VDI, десктопных и веб-приложениях по RADIUS, SAML и OpenID Connect

Технологичное мобильное приложение Avanpost Authenticator с контролем безопасности устройства и работы в изолированных инфраструктурах.

Современные факторы аутентификации, включая push, беспарольный вход по QR-коду, TOTP, SMS, E-mail, U2F/WebAuthn и другие методы;

Позиционирование MFA+

AVANPOST

Многофакторная аутентификация с использованием Avanpost MFA+ — простой, надёжный и технологичный способ защиты от компрометации учётных записей и несанкционированного доступа. Avanpost MFA+ является правильным выбором для решения задач 2FA/MFA, потому что:

Быстро разворачивается по инструкции и экономит время администраторов	Не нужно тратить дни и недели на внедрение системы многофакторной аутентификации.
Построен на платформе Avanpost FAM	Avanpost FAM — платформа корпоративной аутентификации сотрудников для крупных, холдинговых и территориально распределённых организаций. За счёт чего Avanpost MFA+ обладает множеством дополнительных возможностей, недоступных классическим 2FA — решениям.
Работает с мобильным приложением Avanpost Authenticator	Больше не нужно искать компромисс при выборе факторов аутентификации. Простота, удобство, многофакторность, безопасность и универсальность — и всё это в одном мобильном аутентификаторе.
Поддерживает все современные методы подтверждения доступа	Push, QR, усиленный TOTP, Яндекс.Ключ, Google Authenticator, Microsoft Authenticator, аппаратный TOTP, SMS, E-mail, сертификат, Kerberos.

Позиционирование MFA+

AVANPOST

Многофакторная аутентификация с использованием Avanpost MFA+ — простой, надёжный и технологичный способ защиты от компрометации учётных записей и несанкционированного доступа. Avanpost MFA+ является правильным выбором для решения задач 2FA/MFA, потому что:

Один MFA+ для всех корпоративных приложений и систем	Поддерживает все стандартные технологии интеграции: RADIUS, SAML, OpenID Connect, OAuth, LDAP (MS AD, Avanpost DS, FreeIPA, OpenLDAP, ALD Pro), Logon-провайдеры для Windowsи Linux и др.
Экономит нервы и силы технической поддержки вашей организации	Сотрудники автоматически получают инструкции по онбордингу, могут самостоятельно управлять своими аутентификаторами через личный кабинет и сбрасывать доменный пароль с проверкой MFA без создания лишних заявок в техподдержку.
Удобное администрирование	Забудьте о правке бесчисленного множества конфигурационных файлов вашего прежнего 2FA-решения. Настройка всех интеграций выполняется через удобную административную консоль MFA+.
Разворачивайте там, где удобно	Поддерживает установку на все современные операционные системы из deb, rpm-пакетов, docker-контейнеров.

Архитектура системы

AVANPOST

Серверная часть состоит из минимума обязательных компонентов:

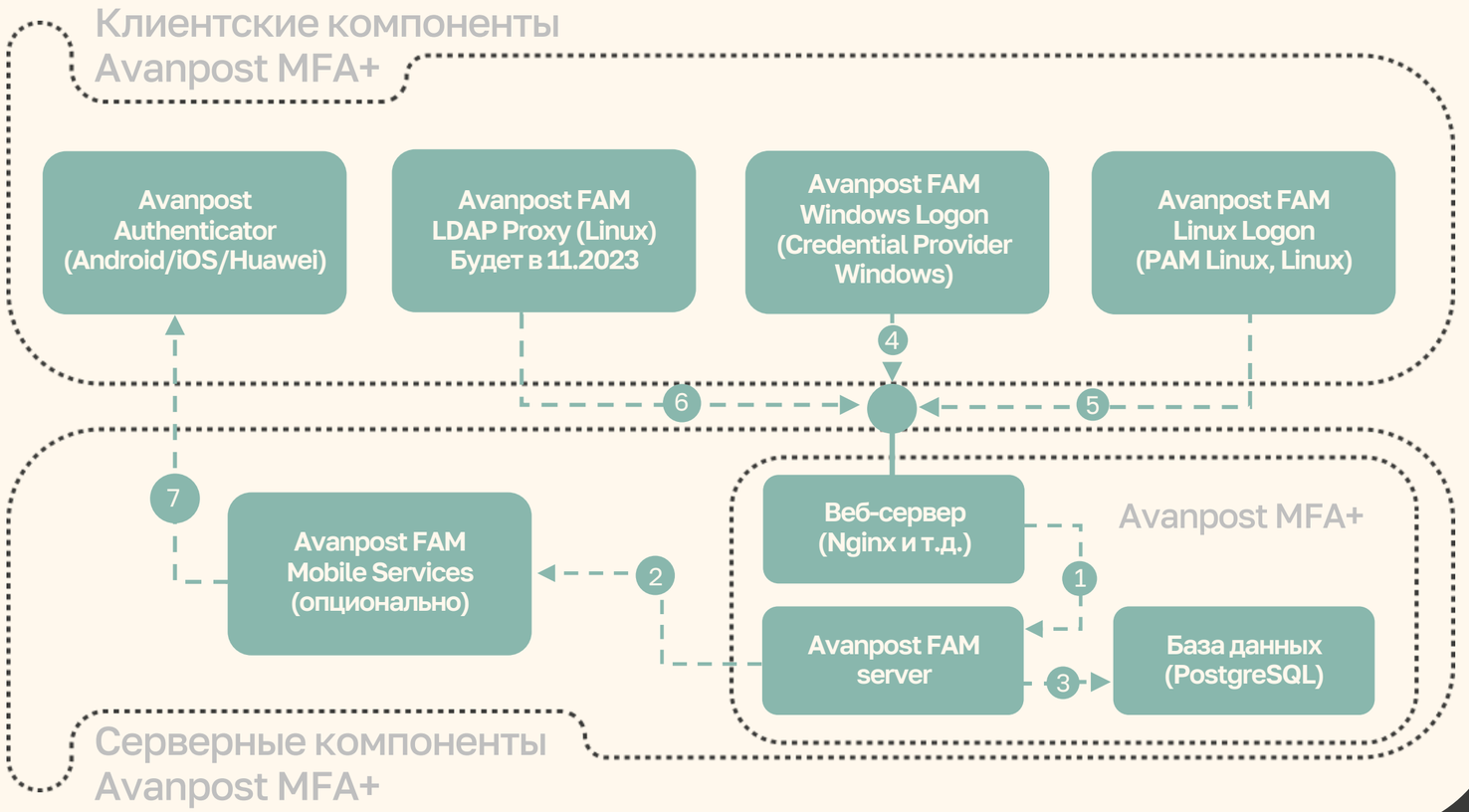
- Avanpost FAM Server
- База данных PostgreSQL
- и набор опциональных:
  Avanpost FAM Mobile Services.

Клиентская часть состоит из опциональных компонентов:

- Avanpost Authenticator
- Avanpost FAM Linux Logon
- Avanpost FAM Windows Logon
- Avanpost FAM LDAP Proxy

Также:

- Использует компоненты из того же набора поставки, что и Avanpost FAM.
- Реализует основные протоколы (OpenID Connect, SAML, RADIUS) встроенными средствами без дополнительных компонентов.
- Серверные компоненты штатно поддерживают кроссплатформерность без JVM и прочих сред выполнения, так как написаны на Golang.



Простое и быстрое развёртывание под вашим контролем

AVANPOST

On-premise – не значит сложно. Avanpost MFA+ быстро и просто устанавливается в любой современной инфраструктуре, что сопоставимо со сложностью установки on-premise-компонентов любого cloud-решения по двухфакторной аутентификации.

Не зависит от внешних обстоятельств. Avanpost MFA+ не зависит от внешних сервисов и находится на 100% под контролем вашей команды. А возможность применения в условиях полной сетевой изоляции позволяет развернуть MFA в самых требовательных к безопасности инфраструктурах.

Больше удобства для администраторов. Настройка параметров интеграции с приложениями выполняется через административную консоль и не требует установки и ручной настройки конфигурационных файлов бесчисленного множества адаптеров и агентов в инфраструктуре.

Готов ко всему. Avanpost MFA+ не привязан к какой-либо платформе и может быть установлен в любой современной ОС. Поддержка контейнеров позволяет использовать MFA в Docker и Kubernetes. Автоматизированная установка через deb и rpm пакеты позволяет максимально упростить процесс.

Рекомендуемые операционные системы:

- Astra Linux;
- Alt Linux;
- RedOS;
- RHEL;
- Oracle Linux;
- CentOS;
- Debian.

Форматы установочных файлов:

- rpm-пакеты;
- deb-пакеты;
- docker-контейнер;
- tar.gz-архив (linux);
- zip-архив (win).

Применяются свободные инфраструктурные компоненты корпоративного уровня без лишних зависимостей:

- Nginx;
- СУБД PostgreSQL, в том числе поддерживаются сертифицированные редакции;

и всё.

Быстрая установка и запуск системы:

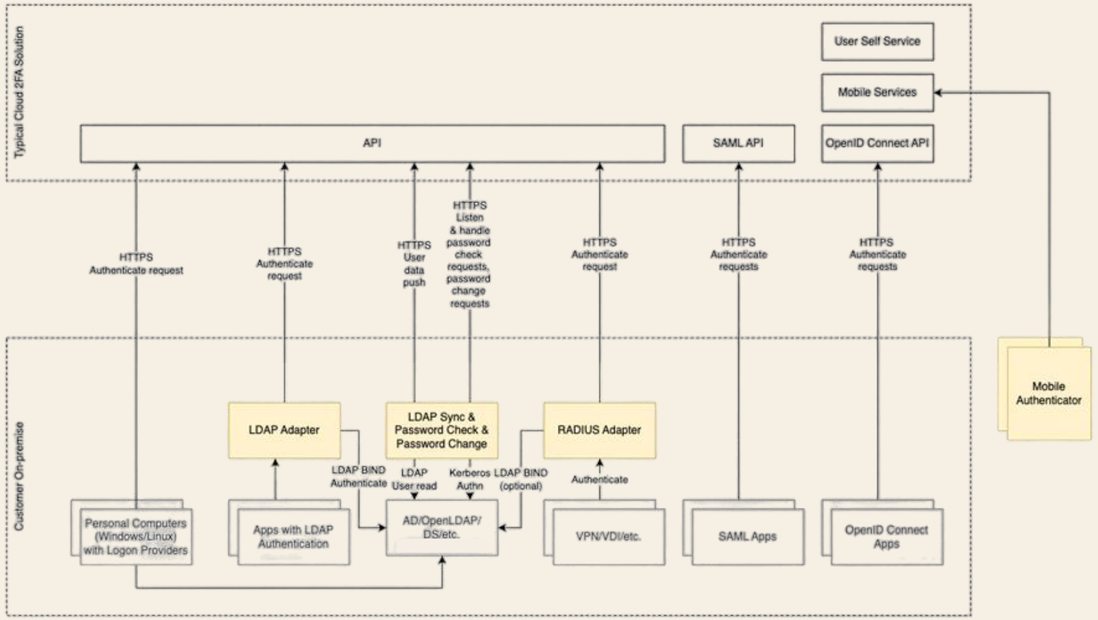
- Общедоступная документация;
- Встроенные установщики (deb, rpm, msi);
- Инструкции по установке и настройке;
- Есть инструкции по интеграции с рядом прикладных систем.

AVANPOST

vs.

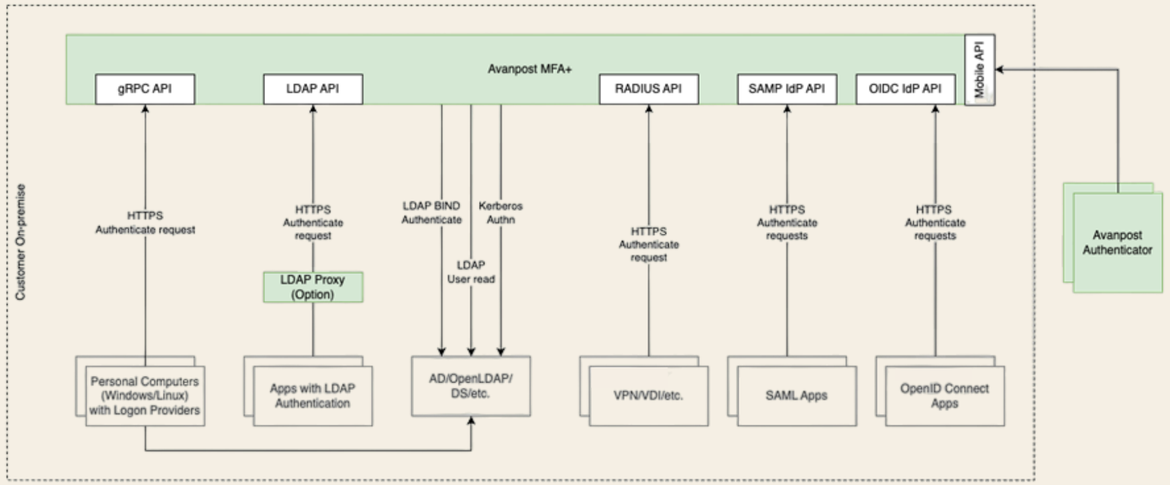
Абстрактный облачный 2FA

- Предполагает установку и настройку в on-premise набора компонентов-адаптеров.
- Требует отдельного конфигурирования и сопровождения каждого развёрнутого компонента-адаптера.
- Требует обширного сетевого взаимодействия через интернет.
- Не требует обслуживания БД.



Avanpost MFA+

- Предполагает установку и настройку в on-premise от 1 компонента.
- Конфигурирование и управление сконцентрировано в рамках одного компонента.
- Допускает ограниченное сетевое взаимодействие через интернет.
- Требует обслуживания БД.



Мобильное приложение Avanpost Authenticator

01 Технологичное мобильное приложение **Avanpost Authenticator** с контролем безопасности устройства и суперспособностью работы в изолированных инфраструктурах.

02 **Методы, предоставляемые Avanpost Authenticator, применимы для безопасной аутентификации во все типы информационных систем:**

- Веб-приложения, сайты и порталы (OpenID Connect, OAuth 2.0, SAML)
- десктопных приложений
- инфраструктурных сервисов (VPN, VDI и RPD, подключаемых через RADIUS)
- рабочих станций и серверов под управлением Windows (Credential Provider) и Linux (PAM Linux)

03 **Avanpost Authenticator - единственное на рынке приложение поддерживает сразу 3 режима входа:**

- TOTP (решена проблема с перехватом секрета через QR код). Есть возможность динамически менять сложность кода, при этом пользователю не нужно проходить процесс перепривязки;
- Push – уведомление
- Вход по QR-коду

04 Усиленный TOTP, используемый для вычисления OTP-кодов в мобильном приложении Avanpost Authenticator, защищён от классической атаки перехвата секрета путём кражи QR-кода привязки TOTP.

05 Особое внимание при создании Avanpost Authenticator было уделено вопросам безопасности размещения в инфраструктуре заказчика. За счет своей архитектуры приложение продолжит функционировать даже в случае недоступности сервисов Google Cloud Messaging и Apple Push Notification Services, предоставляющих стандартные сервисы push-запросов в Android и iOS.

06 Аутентификатор Avanpost умеет проверять настройки и параметры мобильного приложения и параметры самого мобильного устройства с точки зрения защиты PIN-кодом, биометрией, параметров формирования OTP-кода.

07 Универсальная аутентификация с подтверждением при помощи одного мобильного приложения Avanpost Authenticator в рабочих станциях и серверах, VPN, VDI, десктопных и веб-приложениях по RADIUS, SAML и OpenID Connect.

Мобильное приложение

Поддерживаемые платформы:

- Android;
- iOS;
- Huawei.

Методы подтверждения:

- Push, в том числе без доступа в интернет для изолированных инфраструктур;
- Беспарольный вход по QR, в том числе для рабочих станций и серверов;
- Усиленный TOTP с защищённой передачей секрета без возможности компрометации QR-кода.

Функции контроля/compliance мобильного устройства:

- Защита приложения PIN-кодом и его длина
- Защита приложения биометрией;
- Алгоритм вычисления TOTP и длины OTP-кода;
- Контроль наличия root/jailbreak;
- Контроль установки приложения из не доверенных источников.

Независимость функций приложения от облачных сервисов

- Отсутствуют какие-либо промежуточные сервисы между Avanpost Authenticator и Avanpost MFA+, а взаимодействие мобильного приложения выполняется напрямую без сторонних облачных сервисов;
- Онлайн-запросы подтверждения доступа могут работать без сервисов Google, Apple и Huawei;
- Оффлайн-аутентификация по OTP-кодам доступна при отсутствии связи на мобильном устройстве.

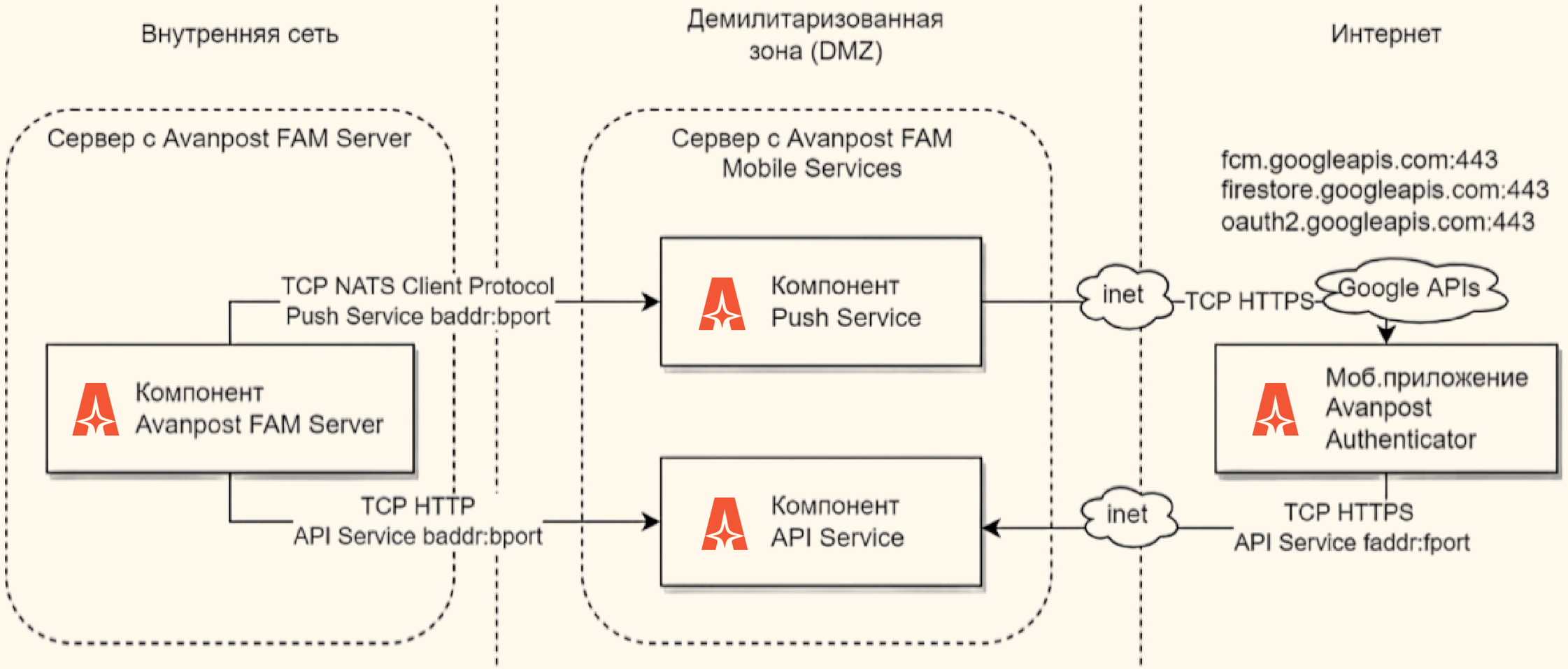
Магазины приложений:

- Apple AppStore;
- Google Play;
- RuStore;
- Huawei AppGallery.

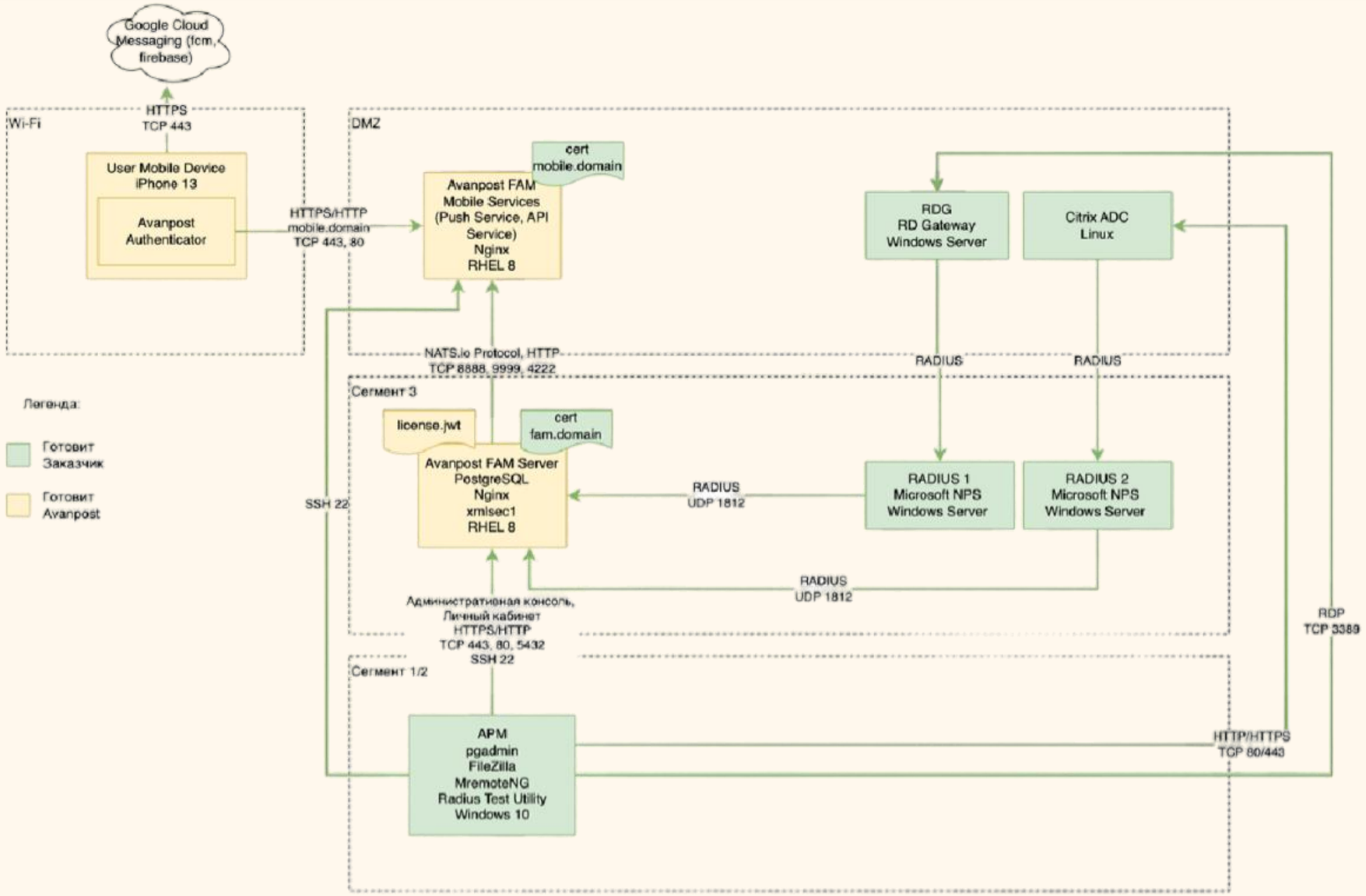
Функции поддержки пользователей:

- Предоставление пользователю информации о технической поддержке организации;
- Журнал запросов и уведомлений
- Отладочный режим с возможностью сбора диагностической информации для последующего предоставления службе технической поддержки организации;
- Уведомления пользователей прямо в мобильном приложении Avanpost Authenticator о событиях смены пароля и т.д.

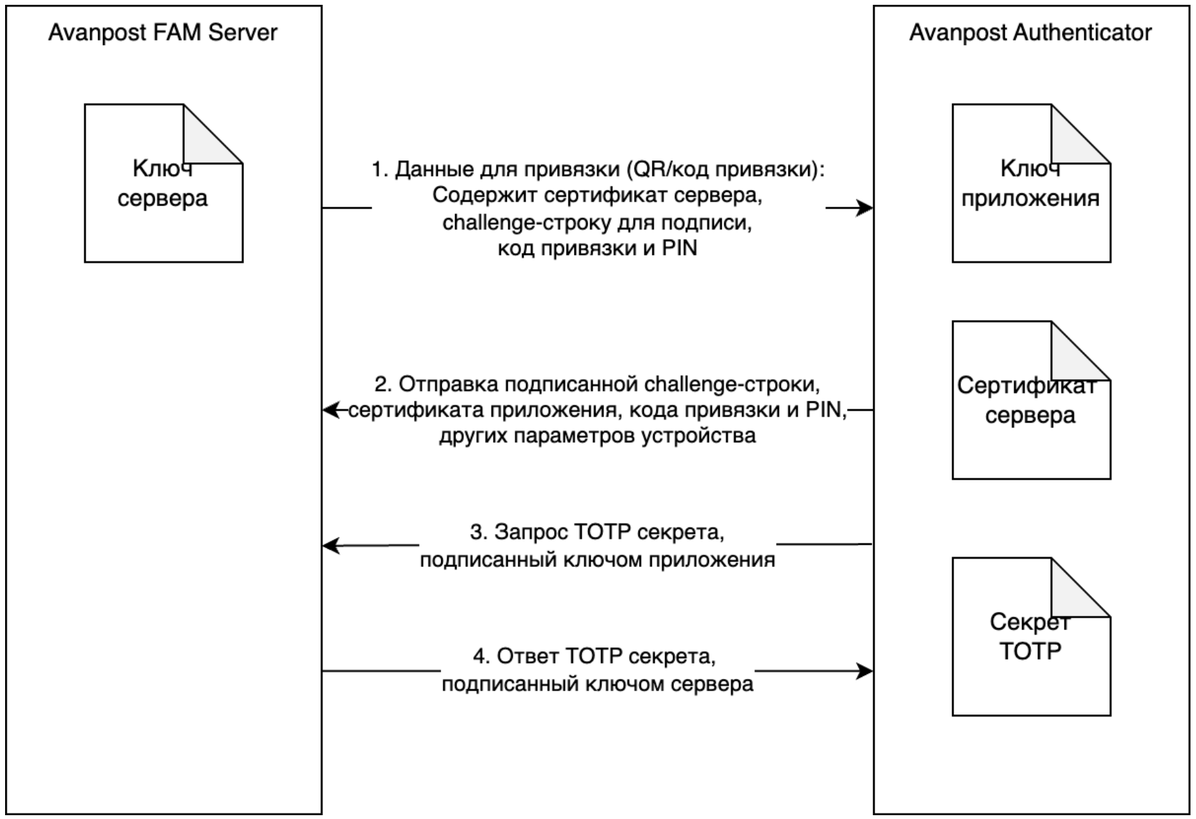
Схема размещения Avanpost Authenticator



Пример изолированного размещения



Защита привязки Avanpost Authenticator



- Взаимодействие мобильного приложения и работает в рамках TLS (при правильном размещении)
- Сервер при привязке передаёт мобильному приложению свой сертификат
- Клиент выпускает свой ключ и отдаёт серверу свой сертификат, а также подписанную challenge-строку
- Последующие запросы мобильного приложения к серверу подписываются ключом приложения и проверяются сервером
- Последующие ответы сервера подписываются ключом сервера и проверяются мобильным приложением

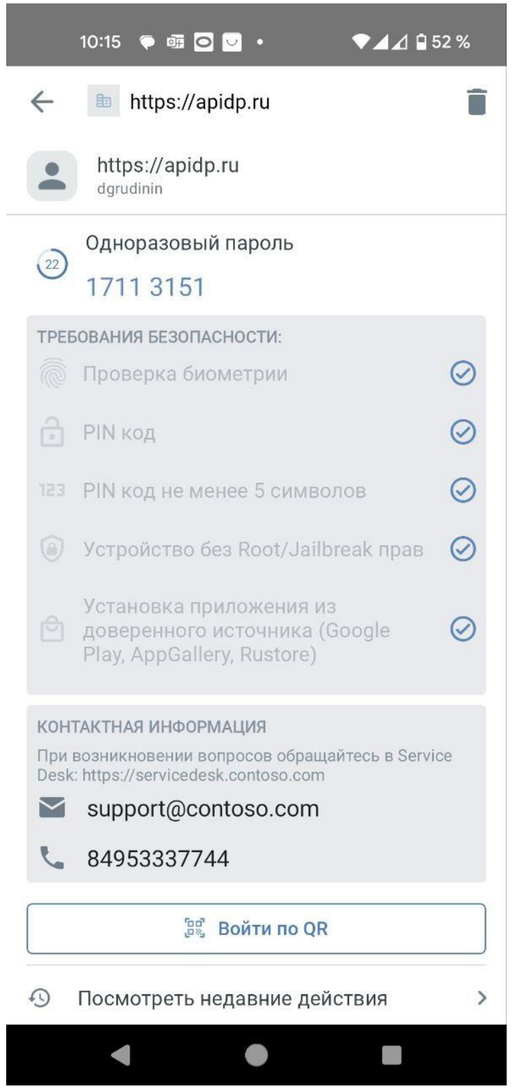
Контроль параметров устройства с Avanpost Authenticator

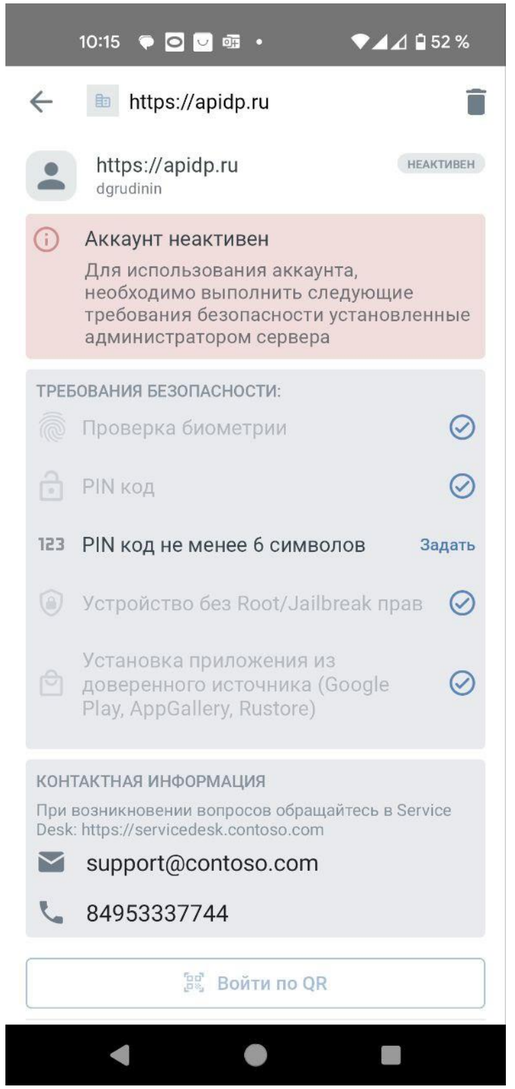
Требования безопасности к мобильному аутентификатору

Пин-код приложения должен быть установлен	☑
Минимальная длина пин-кода	5
Вход в приложение по биометрии должен быть настроен	☑
Длина одноразового пароля (TOTP)	8
Алгоритм одноразового пароля (TOTP)	○ SHA1 ○ SHA256 ◉ SHA512
Ограничить работу приложения на устройствах с root-доступом	☑
Ограничить работу приложения при установке из недоверенного источника	☑

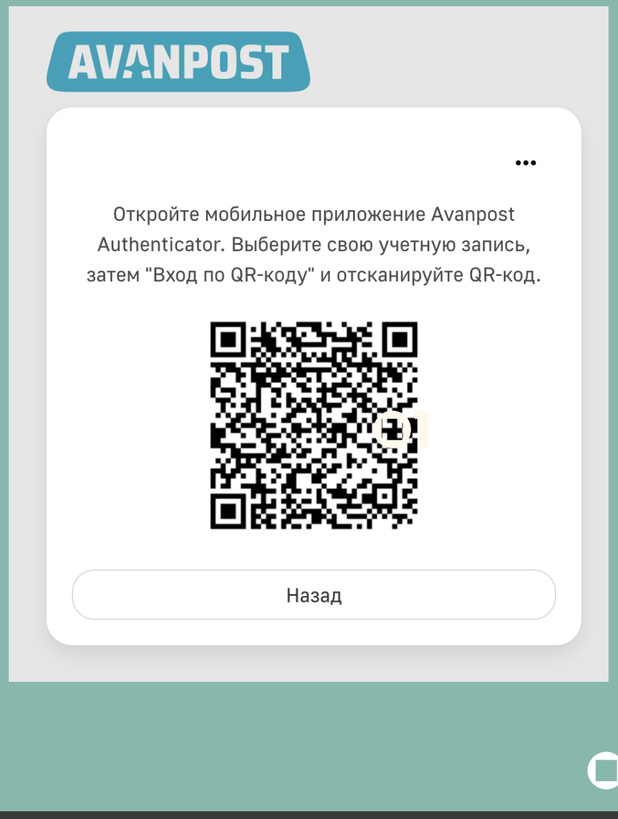
Контактная информация

Email службы технической поддержки	support@contoso.com
Телефон службы технической поддержки	84953337744
Сообщение для пользователей	При возникновении вопросов обращайтесь в Service Desk: http

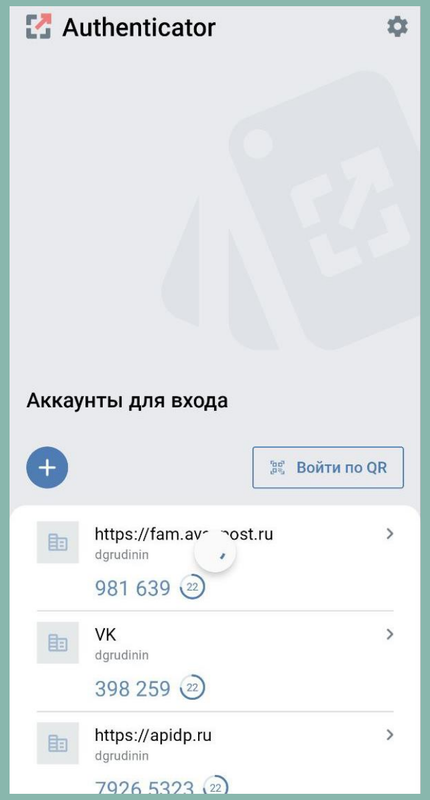




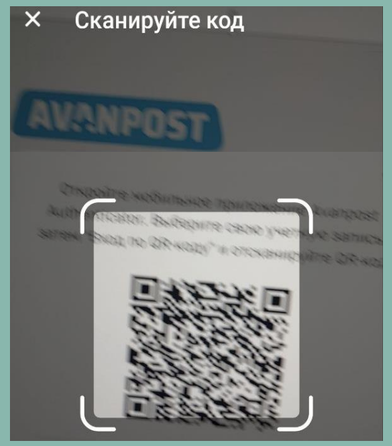
Вход по QR с Avanpost Authenticator



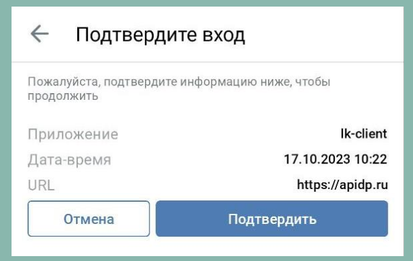
01



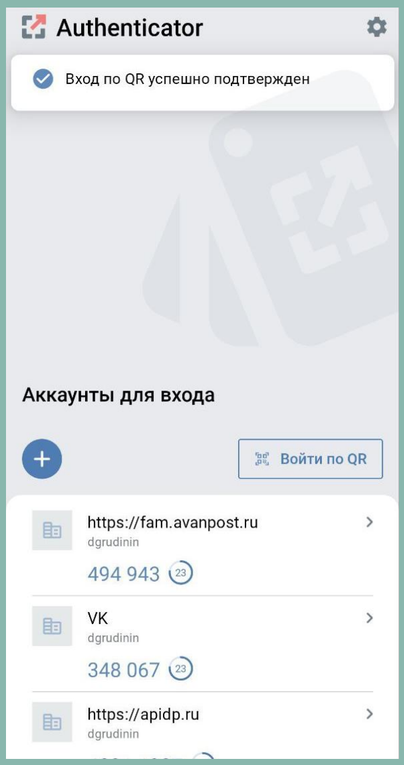
02



03



04



05

Современные факторы аутентификации

Настраивайте самостоятельно любые интеграции с помощью сертифицированных партнёров или собственных ИТ-специалистов.

Avanpost MFA поддерживает все необходимые общепринятые стандарты в области аутентификации, предоставляя невероятную гибкость подключения любых приложений, будь то RADIUS, SAML или OpenID Connect.

Вы можете воспользоваться нашими готовыми решениями для самостоятельного обеспечения адаптивной MFA для рабочих станций и серверов Linux/Windows, VPN- и VDI-решений, корпоративных десктопных и веб-приложений.

AVANPOST

Аванпост предлагает самый широкий ассортимент факторов на рынке:

- Вход по QR через мобильное приложение;
- Push в мобильное приложение;
- Усиленный OTP в мобильном приложении;
- TOTP программный;
- TOTP аппаратный;
- FIDO WebAuthn/U2F;
- Telegram;
- SMS;
- E-mail;
- Kerberos
- Сертификат.

Функции безопасности

- Настраиваемая временная блокировка аккаунта при обнаружении попыток подбора пароля.

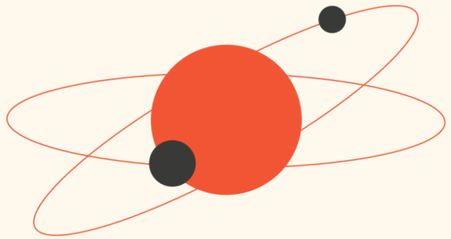
- Настраиваемая временная блокировка фактора или аккаунта при обнаружении попыток подбора:
  - OTP-кода в рамках фактора SMS OTP;
  - OTP-кода в рамках фактора E-mail OTP;
  - OTP-кода в рамках фактора TOTP.

- Ограничение количества одновременных активных сессий на одну учётную запись:
  - В целом по системе;
  - В рамках конкретного приложения.

- Автоматическая блокировка неиспользуемых учётных записей

- Мощные парольные политики с чёрным списком, контролем срока действия

- Настраиваемые требования к формату логина



Самообслуживание с управлением своими аутентификаторами, профилем и паролем через удобный интерфейс администратора

Проработанные пользовательские сценарии

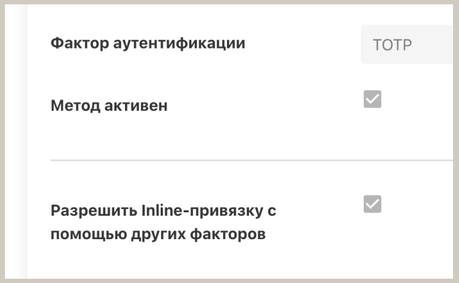
✦ Онбординг

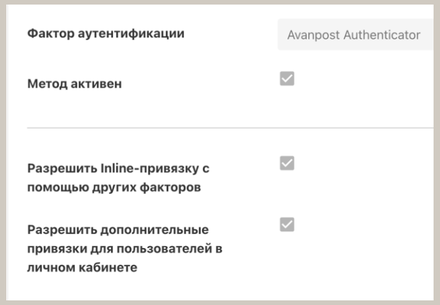
Пользователь при получении учётной записи получает письмо с необходимыми инструкциями для самостоятельной настройки

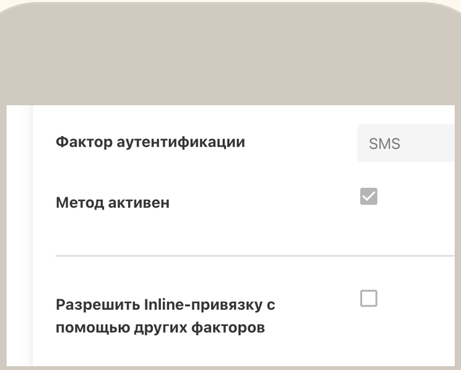
✦ Уведомление

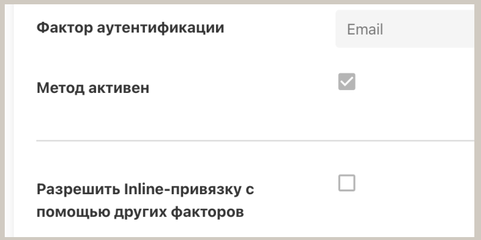
- Самостоятельное управление аутентификаторами
- Функции восстановления доступа

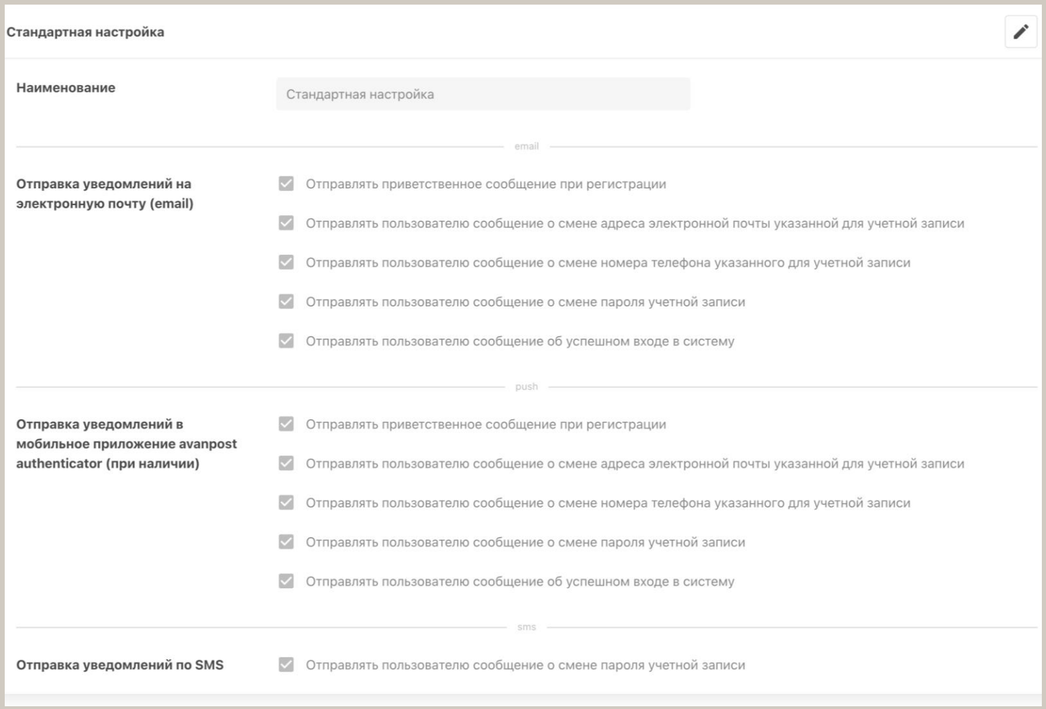
Онбординг и уведомления











Усиленная аутентификация в рабочих станциях и серверах, VPN, VDI, десктопных и веб-приложениях по RADIUS, SAML и OpenID Connect

Avanpost MFA поддерживает все необходимые общепринятые стандарты в области аутентификации, предоставляя невероятную гибкость подключения любых приложений, будь то RADIUS, SAML или OpenID Connect.

01

Вы можете воспользоваться нашими готовыми решениями для самостоятельного обеспечения адаптивной MFA для рабочих станций и серверов Linux/Windows, VPN-и VDI-решений, корпоративных десктопных и веб-приложений.

02

Надёжная аутентификация важна не только для удалённого доступа по VPN, поскольку злоумышленник может быть обыкновенным сотрудником вашей компании. Решение Avanpost MFA+ обеспечивает адаптивной многофакторной аутентификацией все самые критичные элементы корпоративной инфраструктуры - веб-приложения, тонкие клиенты, десктопные приложения, рабочие станции и сервера.

03

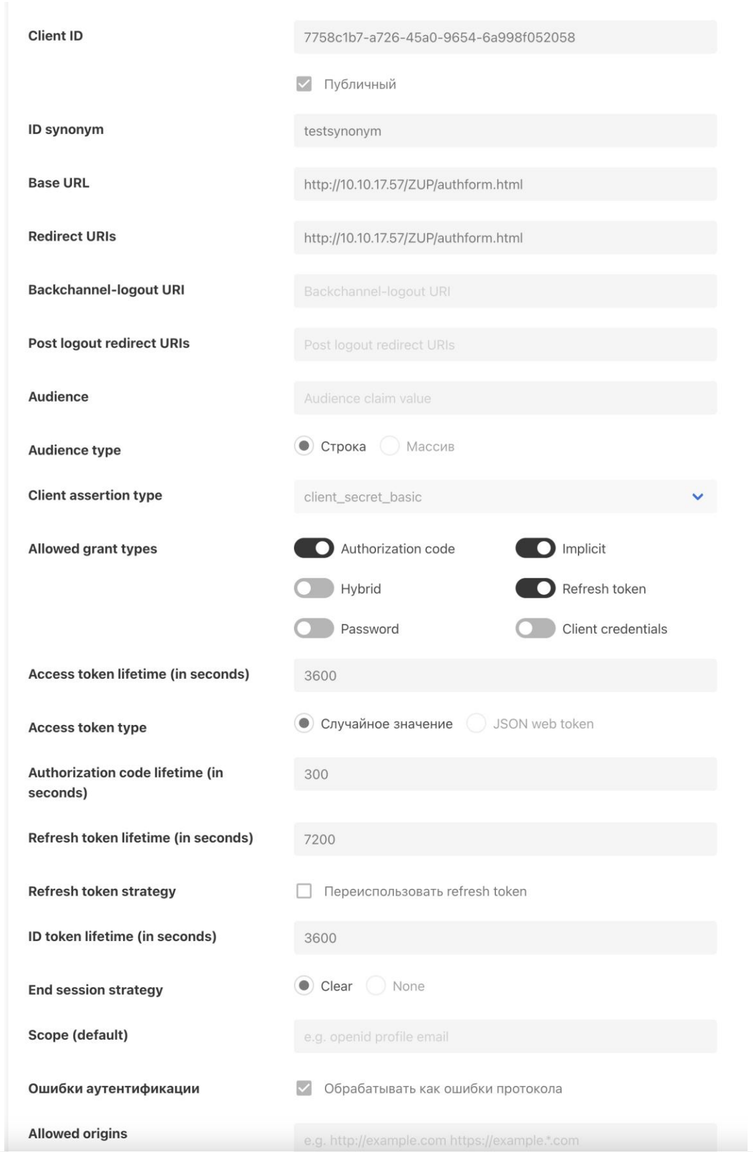
За счёт использования развитых реализаций стандартизированных протоколов RADIUS, SAML и OpenID Connect, а также богатого опыта применения этих протоколов, унаследованного от Avanpost FAM, MFA+ позволяет с лёгкостью подключить основной пул ваших информационных систем.

04

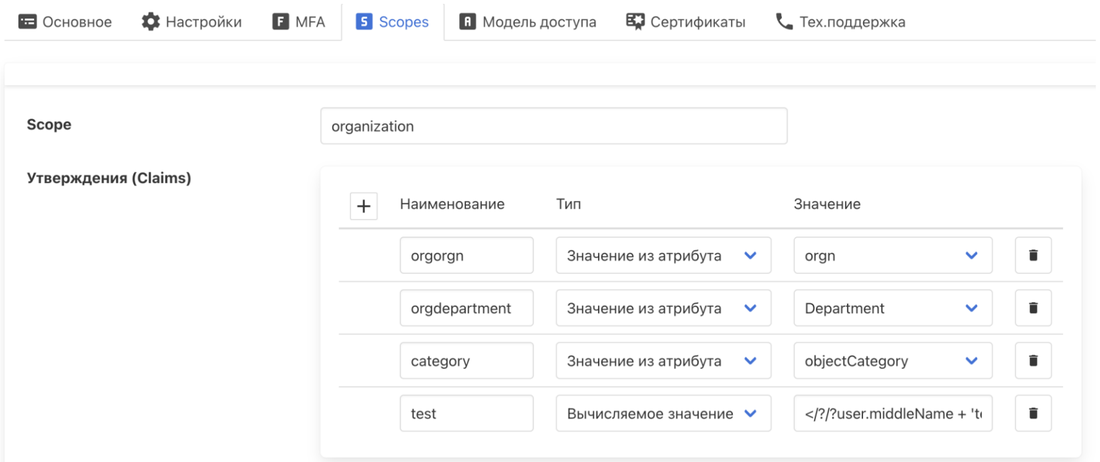
А за счёт удобной административной консоли интеграция ваших приложений будет по-настоящему простой и удобной.

05

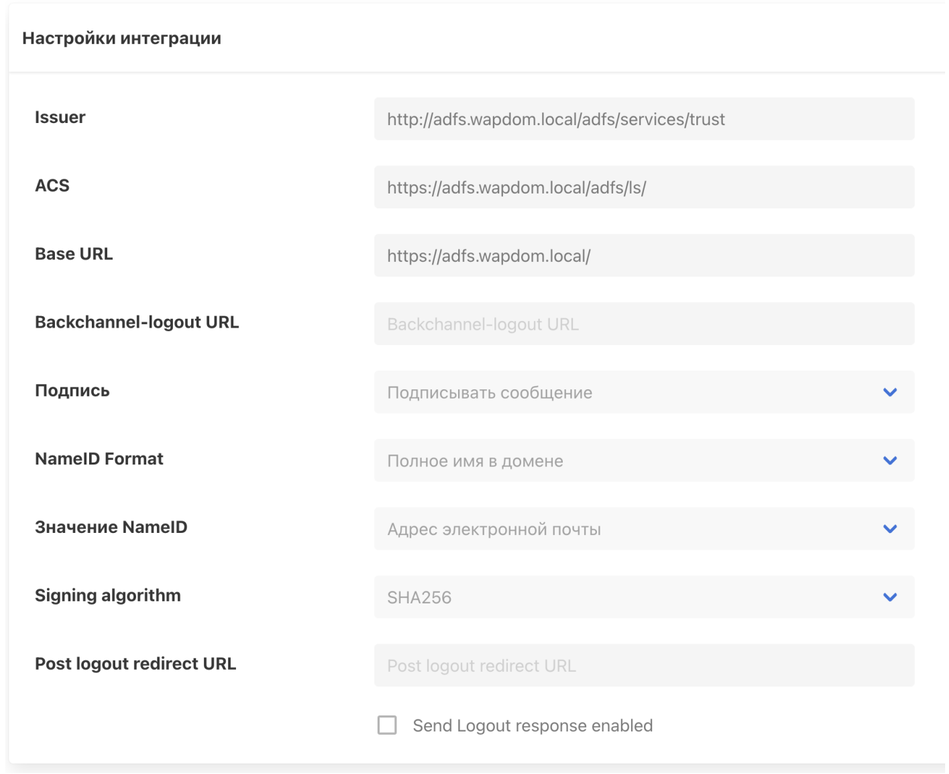
Особенности OpenID Connect/OAuth



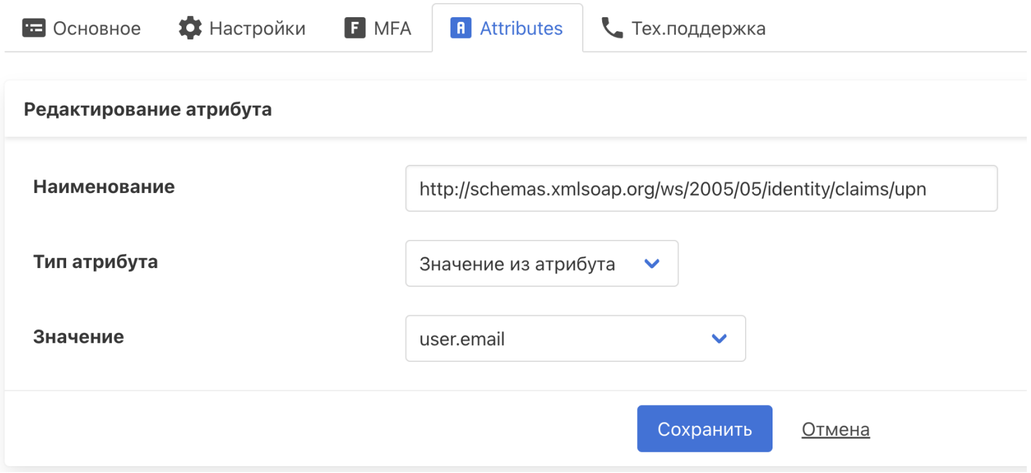
- Поддержка публичных/не публичных клиентов
- Поддержка CORS для мобильных приложений/SPA
- Поддержка современных Grant Types
- Гибко тюнингуемые параметры срока действия всех токенов и Authorization Code
- Гибко настраиваемый состав scopes и claims, в том числе с возможностью динамической модификации значения
- Поддержка Backchannel Logout



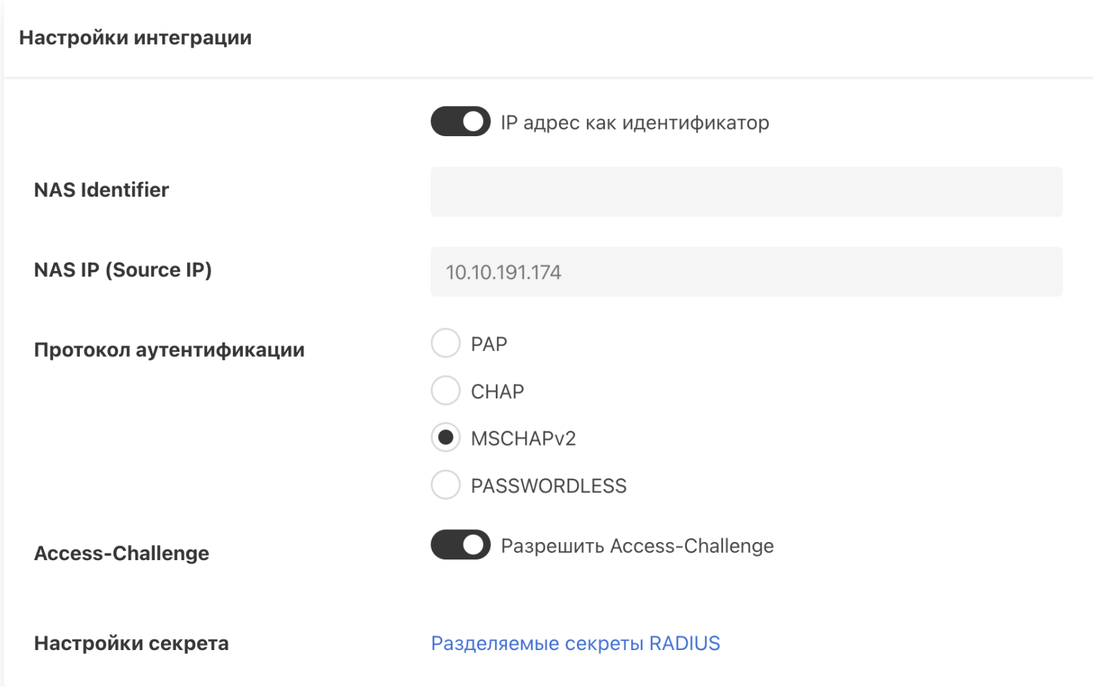
Особенности SAML



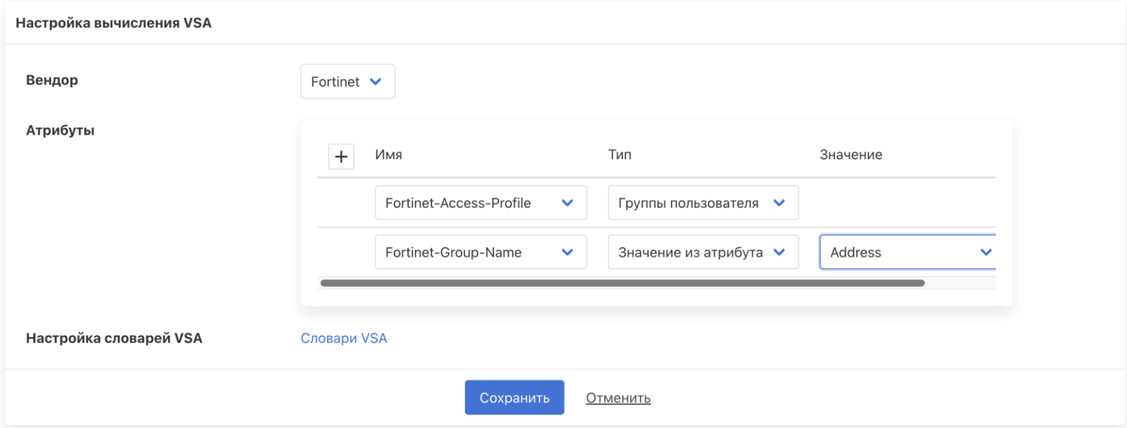
- Гибко настраиваемый состав SAML Assertions, в том числе с возможностью динамической модификации значения
- Поддержка Backchannel Logout



Особенности RADIUS



- Поддержка PAP, CHAP, MSCHAPv2
- Поддержка Passwordless-режима
- Поддержка Vendor-Specific-атрибутов



Поддерживаемые MFA+ системы

Примеры инструкций по интеграции прикладных систем, подключаемых по стандартным протоколам:

OAuth 2.0/OpenID Connect

- Настройка MFA/SSO для 1С:Предприятие 8.3.14 и выше (OpenID Connect)
- Настройка MFA/SSO для Atlassian Confluence Server
- Настройка MFA/SSO для Atlassian Jira Server
- Настройка MFA/SSO для GitLab
- Настройка MFA/SSO для Grafana

SAML 2.0

- Настройка 2FA/MFA для Citrix Virtual Apps and Desktops, Citrix XenApp, Citrix XenDesktop без Citrix FAS
- Настройка MFA/SSO для Atlassian Confluence Server
- Настройка MFA/SSO для Atlassian Jira Server
- Настройка MFA/SSO для CRM Creatio (Terrasoft bpm'online)
- Настройка MFA/SSO для Google Workspace
- Настройка MFA/SSO для Р7-Офис

RADIUS

- Настройка 2FA для CheckPoint VPN
- Настройка 2FA для Linux SSH
- Настройка 2FA для Microsoft VPN
- Настройка 2FA для Mikrotik VPN
- Настройка 2FA для OpenVPN
- Настройка 2FA для Remote Desktop Gateway/RD Gateway
- Настройка 2FA для VMware Horizon View
- Настройка 2FA/MFA для Cisco AnyConnect, Cisco ASA, Cisco ASAv

Примеры инструкций по интеграции прикладных систем, подключаемых посредством Logon-провайдеров:

Credential Provider

- Настройка MFA для Windows Desktop/Server при подключении по RDP
- Настройка MFA для APM под управлением Windows Desktop

PAM Linux

- Настройка 2FA для Linux SSH

- Установка FAM Linux Logon в Astra Linux

Сравнение решений на рынке

AVANPOST

Критерий	MFA+	Indeed AM	Multifactor	Аладдин (JAS)
Модель	**On-premise**	**On-premise**	**Cloud**	**On-premise**
Поддерживаемые платформы	**Linux, Windows Server, UNIX**	**Windows Server**	**-**	**Windows Server**
Механизмы вычисления сценария	**MFA с динамически вычисляемыми многошаговыми сценариями**	**2FA с настройкой второго фактора по политике**	**2FA с настройкой второго фактора по политике**	**2FA с настройкой второго фактора по политике**
Контексты для подбора факторов	**7 контекстов:** • Целевое приложение; • Атрибуты профиля пользователя; • Группы пользователя; • Роли пользователя; • Проверенные в рамках сессии факторы; • Открытые в рамках сессии приложения; • Сетевые параметры запроса.	**2 контекста:** • Целевое приложение; • Группы пользователя;	**3 контекста:** • Целевое приложение; • Группы пользователя; • Сетевые параметры запроса.	**2 контекста:** • Целевое приложение; • Группы пользователя.
Методы аутентификации	**Ассортимент из 11 факторов:** • Вход по QR; • Push в мобильное приложение; • Защищённый OTP в мобильном приложении; • TOTP программный; • TOTP аппаратный; • FIDO WebAuthn/U2F; • Telegram; • SMS; • E-mail; • Kerberos; • Сертификат.	**Ассортимент из 7 факторов:** • Push в мобильное приложение, • E-mail, • HOTP, • SMS, • TOTP программный, • Telegram, • Секретное слово.	**Ассортимент из 7 факторов:** • Push в мобильное приложение, • TOTP программный, • TOTP аппаратный, • Telegram, • SMS, • Звонок, • FIDO WebAuthn/U2F.	**Ассортимент из 7 факторов:** • Push в мобильное приложение; • Защищённый OTP в мобильном приложении; • TOTP программный; • TOTP аппаратый; • HOTP; • SMS; • FIDO WebAuthn/U2F.
Число аутентификаторов у пользователя	Несколько одного вида	Несколько одного вида	Один одного вида	Один одного вида
Администрирование параметров приложений	Административная консоль	Конфигурационные файлы	Конфигурационные файлы	Конфигурационные файлы
Методы интеграции приложений	**6 методов:** • RADIUS; • OpenID Connect/OAuth; • SAML; • Windows Logon (собственный Credential Provider); • Linux Logon (собственный PAM Linux-модуль); • LDAP Proxy (планируется 11.2023).	**4 метода:** • RADIUS; • OpenID Connect/OAuth; • SAML; • Windows Logon (собственный Credential Provider).	**6 методов:** • RADIUS; • OpenID Connect/OAuth; • Windows Logon (собственный Credential Provider); • Linux Logon (PAM Linux-модуль из состава FreeRADIUS); • LDAP Proxy; • Прикладная интеграция через плагины к ADFS и т.д.	**3 метода:** • RADIUS; • Windows Logon (собственный Credential Provider); • Прикладная интеграция через плагины к ADFS и т.д.

Что предлагаем заказчикам?

Характеристика	Avanpost FAM	Avanpost MFA+
Целевой заказчик	Организации более 10 000 сотрудников с распределённой инфраструктурой (холдинг, несколько ЦОДов, множество доменов) и большим числом разнородных информационных систем	Организации до 3 000 сотрудников со стандартной[1] корпоративной инфраструктурой в пределах одного ЦОДа с информационными системами, использующими стандартные методы аутентификации
Ключевые функции	IdP, MFA (двухфакторная/многофакторная аутентификация), Single Sign-On (однократный вход), Single Logout (централизованное завершение сессии), авторизация на уровне разрешения/запрета доступа к приложению, делегированная UMA 2.0 авторизация с вычислением прав пользователя в приложении	IdP, MFA (двухфакторная/многофакторная аутентификация)
Методы аутентификации	Password, Avanpost Authenticator, TOTP, SMS, E-mail, смарт-карты (Rutoken, JaCarta), электронная подпись (сертификат), Kerberos, доверенные IdP, FIDO WebAuthn/U2F	Password, Avanpost Authenticator, TOTP, SMS, E-mail, Kerberos[1], FIDO WebAuthn/U2F
Реализация	PROJECT	BOX (+ опционально дополнительные опции, PROJECT)
Лицензирование	Subscription, Perpetual **$$$** от 1 000 до 5 000 от 5 000 до 20 000 от 20 000 до 30 000 30 000 и более	Subscription, Perpetual **$** от 500 до 1 000 от 1 000 до 3 000 от 3 000 до 5 000 5 000 и более
Сертификация ФСТЭК	Сертифицирован по 4 уровню доверия и может быть использован в ИСПДн, ГИС, КИИ и КВО до 1 класса/категории включительно.	Содержится в качестве исполнения в сертификации FAM

[1] - под стандартной доменной инфраструктурой подразумевается не более 2 LDAP-каталогов и не более 2 контроллеров Kerberos (2 keytab-файла)

AVANPOST

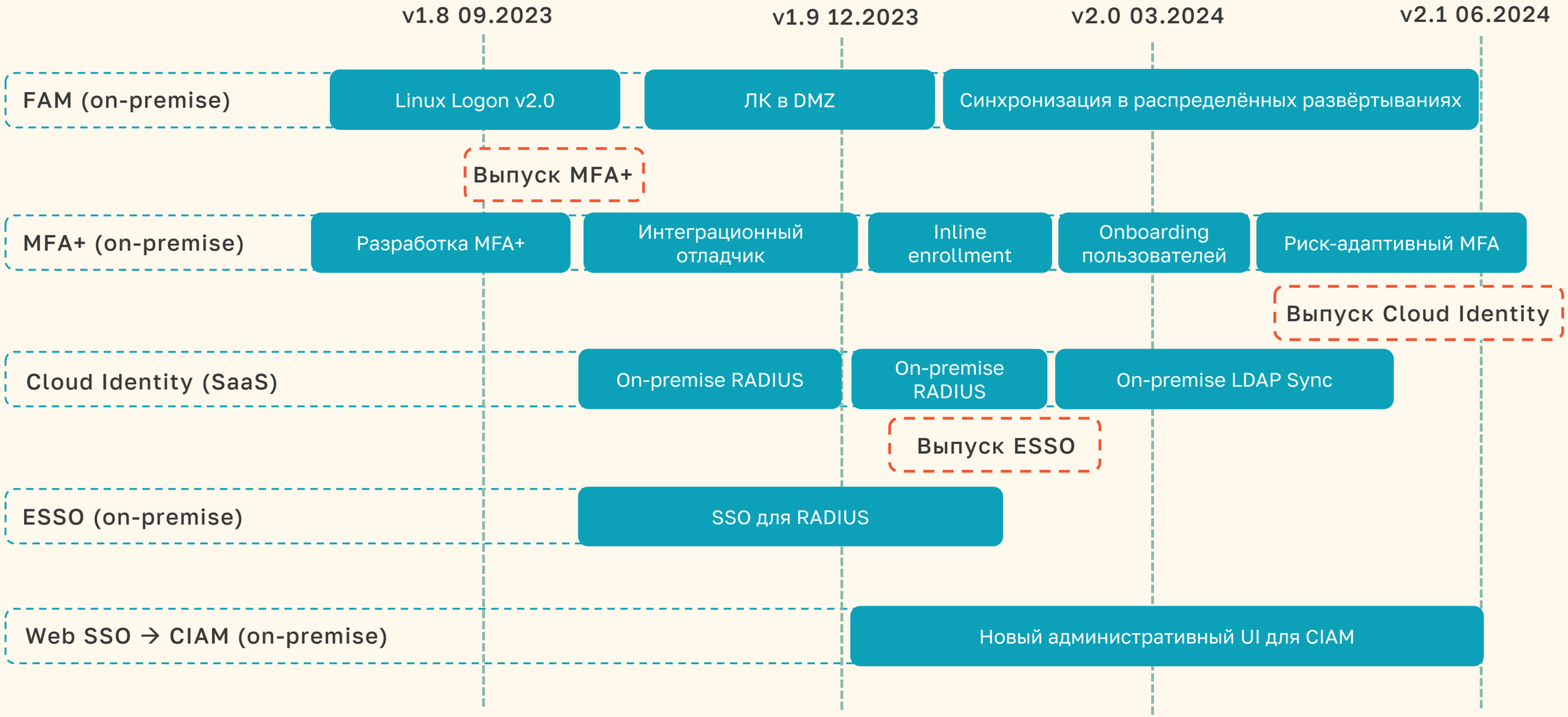
+ Дополнительные опции

MFA +	+1 Reverse-Proxy/ Legacy приложений	Интеграция продукта с одной унаследованной (legasy) корпоративной информационной системой или интеграция продукта с одним обратным прокси-сервером. Тарифицируется за каждое дополнительное подключенное приложение.	Расширение лицензии $	BOX
MFA +	+1 Desktop приложение	Интеграция продукта с одним desktop приложением. Тарифицируется за каждое дополнительное подключенное приложение.	Расширение лицензии $	BOX
MFA +	Управление устройствами	Управление устройствами позволяет организациям администрировать и обслуживать устройства, включая виртуальные машины, физические компьютеры, мобильные устройства и устройства Интернета вещей, является критически важным компонентом стратегии безопасности организации: помогает обеспечить безопасность, актуальность и соответствие устройств политикам организации с целью защиты корпоративной сети и данных от несанкционированного доступа. Модуль на 3 устройства.	Расширение лицензии $	BOX
MFA +	Федерация	Функциональность федерации удостоверений позволяет использовать одни идентификационные данные для нескольких компаний, или распределить систему на несколько экземпляров в рамках единого информационного пространства.	За стороннего провайдера $	BOX
MFA +	Риск-адаптивная аутентификация	Система адаптивной аутентификации на основе анализа рисков для управления входом пользователей в приложения. Модуль на пользователя.	Расширение лицензии $	Project $

Roadmap продуктовой линейки FAM

AVANPOST

Q4’2023-Q3’2024



Общие правила предоставления скидок партнерам

Скидки на лицензии:

Партнерская скидка

На лицензии MFA+ от плана продаж и экспертизы: 8-20%

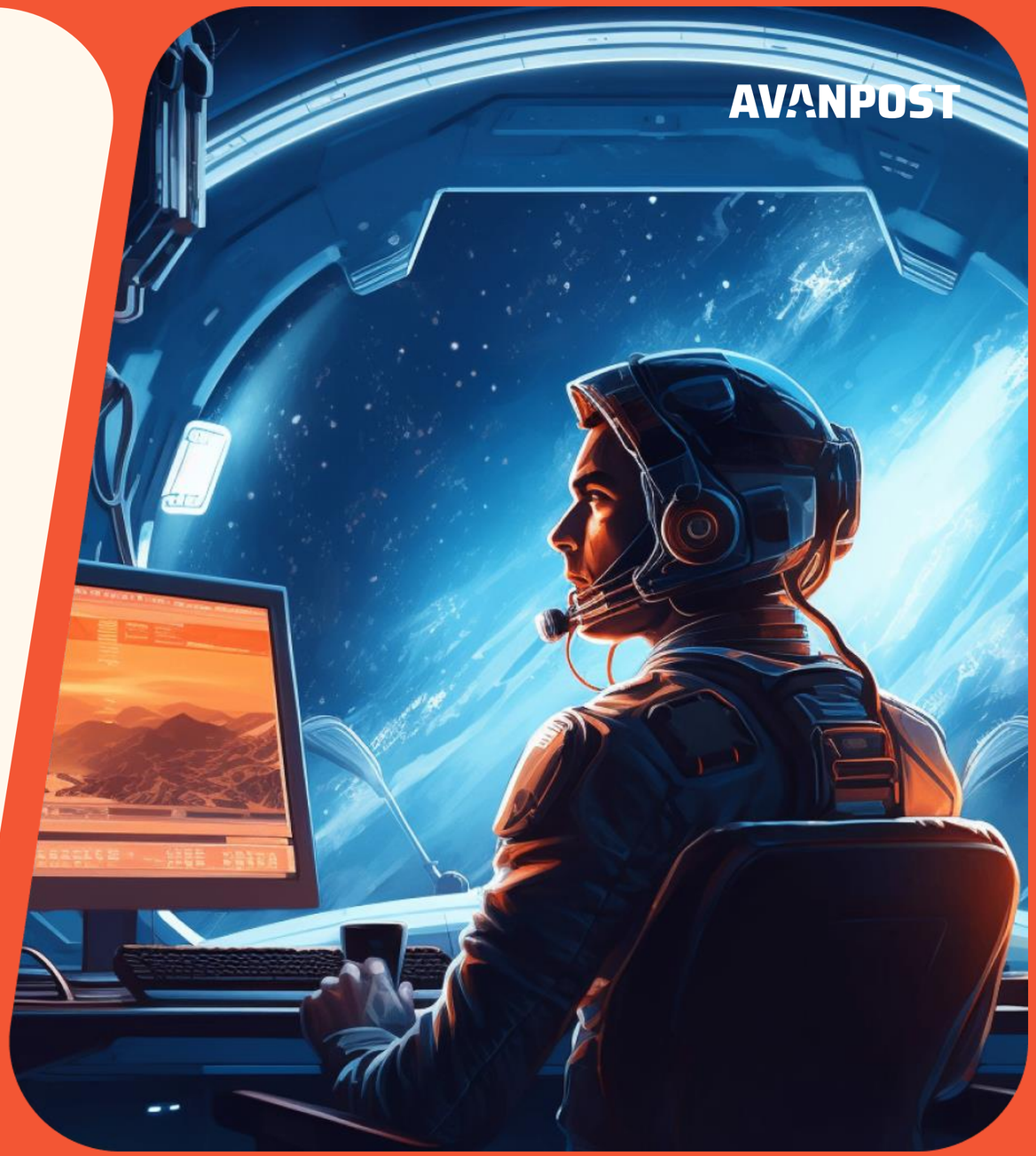
На лицензии FAM от плана и экспертизы: 15-35%

Клиентская скидка

Спец условия от объема покупки
FAM более 30 000 пользователей
MFA+ более 5 000 пользователей

Защита сделки 10%

Внимание: скидка на работы партнеру не предоставляется. Партнерскую скидку нельзя использовать, как клиентскую – это маржа партнера.



AVANPOST

Воспользуйтесь нашими материалами и видео-инструкциями по развертыванию решения MFA+ силами собственных специалистов в течение одного рабочего дня!

01 Сканируй

02 Скачивай

03 Следуй инструкции

СКАНИРУЙ И ПРОБУЙ

Эко-система продуктов Avanpost

AVANPOST

AVANPOST DS
Directory Service

Общая информационная инфраструктура для управления и систематизации ресурсов: тома, папки, файлы, принтеры, пользователи, группы, устройства, телефонные номера и др. объекты.

AVANPOST PAM Privileged Access Management

Система предотвращения несанкционированного привилегированного доступа к критически важным ресурсам.

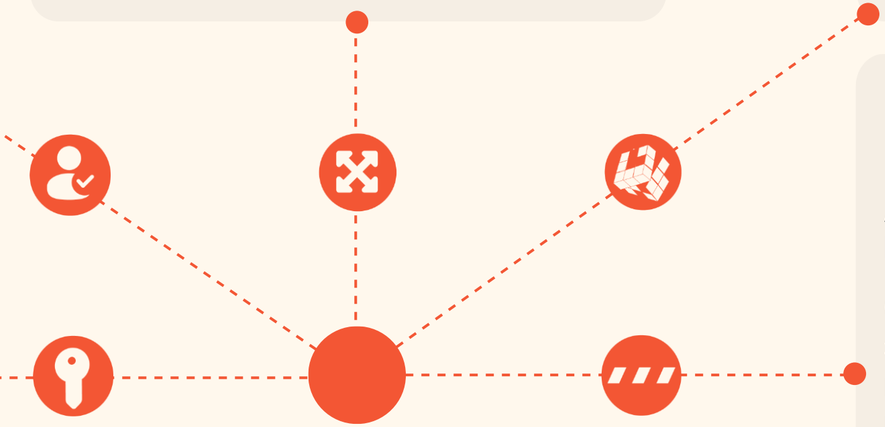
AVANPOST PKI
public key infrastructure

Система управления всеми элементами инфраструктуры открытых ключей из единого центра.

AVANPOST FAM
Federated Access Manager

Современный центр управления многофакторной аутентификацией в корпоративных приложениях с поддержкой федерации удостоверений.

- **Multi-factor Authentication (MFA+)**
  Провайдер многофакторной аутентификации с поддержкой всех современных методов аутентификации, гибкой настройкой факторов через удобный интерфейс администратора
- **Single-Sign-on (SSO)**
- **WEB SSO state**
- **WEB SSO - CIAM**



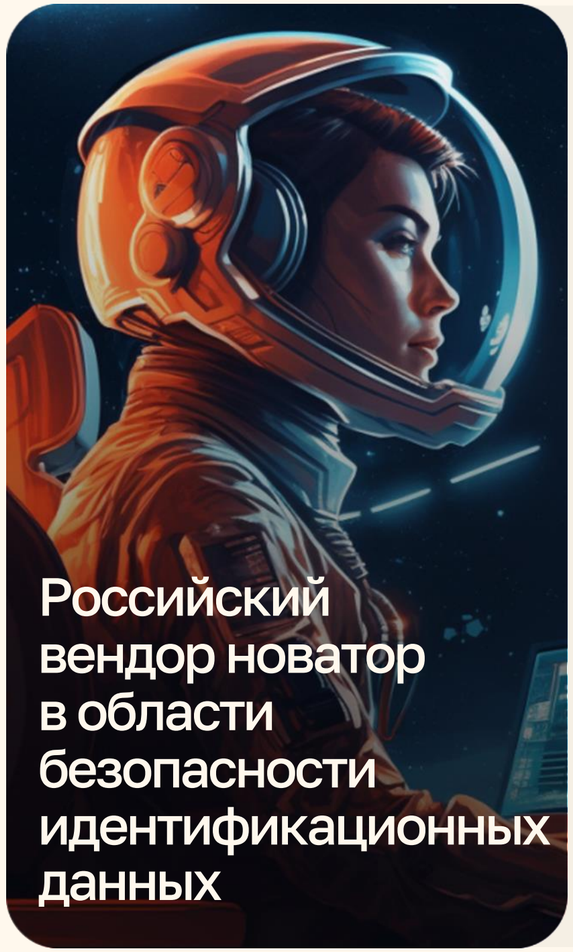
- Облачная версия продукта в рамках базового сервиса ГосТеха
- Облачная версия продукта
- Мобильное приложение

AVANPOST IDM
Identity Management

Система управления учетными записями и доступом к корпоративным ресурсам предприятия.

AVANPOST

Технологические преимущества



Развивает свою экспертизу с 2007 года.

Экспертиза команды и опыт сотен успешных внедрений позволяет решать задачи любой сложности независимо от отрасли и используемых предприятием систем.

Продукты Avanpost включены в реестр отечественного ПО, удовлетворяют требованиям безопасности информации и сертифицированы ФСТЭК, применимы в ГИС, ИСПДн, КИИ, КВО.

Предлагает экосистему управления доступом, построенную на базе собственного программного обеспечения, лучшего в своем классе.

01

Предоставляет своим клиентам мощную легко масштабируемую платформу, позволяющую перейти от фрагментарной стратегии аутентификации и управления доступом к информационным ресурсам к целостному подходу обеспечения безопасности предприятия.

02

Полностью собственная разработка, не зависит от сторонних решений и OpenSource компонент.

03

Отдельные продукты интегрируются друг с другом в многофункциональную экосистему.

04

Руководитель отдела по работе с партнерами

Иванова Надежда

nivanova@avavnpost.ru

Отдел по работе с партнерами

partner@avavnpost.ru

Ведущий разработчик систем аутентификации и управления доступом