CURATOR.IDENTITY product guide

О решении

CURATOR.IDENTITY — решение для управления аутентификацией и безопасным доступом сотрудников, подрядчиков и внешних пользователей, встроенное в облачную экосистему CURATOR.

С помощью CURATOR.IDENTITY компании могут быстро внедрить MFA и SSO, усилить контроль устройств и пользовательских сессий, а затем последовательно развивать архитектуру защищённого доступа — от базовой многофакторной аутентификации до зрелых сценариев Zero Trust.

CURATOR.IDENTITY обеспечивает доступ к веб-приложениям, VPN, корпоративным порталам, инфраструктурным сервисам, а также десктопным и legacy-приложениям. Централизованные политики аутентификации и доступа помогают снизить риски компрометации учётных записей, кражи пользовательских сессий и несанкционированного доступа к критически важным системам.

Какую задачу решает

Современные атаки всё чаще начинаются не со взлома внешнего периметра, а с компрометации учётных записей и пользовательских сессий.

Используя украденные логины и пароли, скомпрометированные токены и активные сессии, а также уязвимые для фишинга механизмы MFA, злоумышленники могут получить доступ к инфраструктуре под видом легитимных пользователей.

Поэтому даже при наличии сетевой защиты, WAF, мониторинга и других средств информационной безопасности сохраняется риск того, что злоумышленник войдёт в корпоративную систему с правами сотрудника, подрядчика или администратора.

CURATOR.IDENTITY помогает снизить этот риск благодаря централизованному управлению доступом, усиленной аутентификации, SSO и контролю пользовательских сессий. Контекстные политики позволяют учитывать пользователя, устройство и параметры запроса, создавая основу для последовательного перехода к архитектуре Zero Trust.

Основные задачи:

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- усиление аутентификации с помощью MFA и отказ от использования пароля как единственного фактора защиты;
- централизованное управление доступом сотрудников, подрядчиков и внешних пользователей;
- защита удалённого доступа к VPN, веб-приложениям, корпоративным порталам и инфраструктурным сервисам;
- внедрение SSO без развёртывания сложной локальной инфраструктуры;
- применение контекстных политик с учётом пользователя, группы, IP-адреса, устройства и сценария доступа;
- контроль пользовательских сессий и снижение риска их компрометации или повторного использования;
- подключение десктопных и legacy-приложений к единой системе аутентификации;
- снижение нагрузки на ИТ-службу и поддержку благодаря единому входу и самостоятельному выполнению типовых операций пользователями;
- последовательное развитие системы управления доступом в соответствии с принципами Zero Trust.

Для кого предназначен

CURATOR.IDENTITY предназначен для компаний, которым важно защищать доступ к корпоративным системам, снижать риск компрометации учетных записей и управлять аутентификацией сотрудников, подрядчиков и внешних пользователей.

Основные пользователи внутри компании

- ИТ-директора;
- руководители ИТ;
- CISO и руководители ИБ;
- администраторы инфраструктуры;
- IAM-инженеры;
- DevOps-команды;
- владельцы корпоративных приложений;
- команды эксплуатации;
- службы поддержки пользователей.

Место решения в экосистеме Curator

CURATOR.IDENTITY расширяет портфель Curator в сторону защиты доступа, идентичности и пользовательских сессий.

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Если базовые решения Curator помогают защищать внешнюю инфраструктуру, фильтровать трафик, обеспечивать доступность публичных ресурсов и выявлять уязвимости, то CURATOR.IDENTITY закрывает другой критичный слой безопасности — доступ пользователей к корпоративным системам.

Таким образом, клиент получает более целостный контур безопасности: не только защиту приложений и инфраструктуры, но и управление безопасным доступом к ним.

Основные преимущества

Быстрый запуск защищенного доступа

CURATOR.IDENTITY позволяет быстро включить MFA и SSO для типовых корпоративных сценариев: VPN, web-приложений, корпоративных порталов и сервисов, подключаемых по стандартным протоколам.

Не нужно начинать с большого on-prem проекта. Базовый запуск можно выполнить в облачной модели, постепенно развивая функциональность.

Развитие защиты в рамках одной платформы

Компания может начать с базового MFA, затем перейти к контекстной аутентификации, Unified SSO, защите сессий, контролю устройств и Zero Trust. Это снижает риск миграций, смены решений и разрозненности инструментов.

Баланс безопасности и удобства

Решение не просто усиливает проверки, а помогает применять их там, где это действительно нужно. Обычные сценарии можно делать удобнее, а критичные — защищать строже.

Поддержка сотрудников и подрядчиков

CURATOR.IDENTITY подходит не только для штатных сотрудников, но и для подрядчиков, внешних пользователей, администраторов и привилегированных учетных записей.

Настоящий SSO для разных сценариев

Решение поддерживает не только web SSO, но и более зрелые сценарии единого входа, включая desktop-, legacy- и инфраструктурные приложения на старших тарифах.

Контроль устройств

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

На более зрелых уровнях платформа позволяет учитывать устройство как фактор доверия: определять устройство, собирать сигналы безопасности, строить профиль и использовать его в политике доступа.

Защита сессий

Технология E-passport и Unified SSO помогают снизить риск перехвата и повторного использования пользовательской сессии.

Гибридная архитектура

Access Bridge позволяет безопасно связать облачную платформу с инфраструктурой клиента, не публикуя внутренние сервисы наружу.

Прозрачный рост от MFA к Zero Trust

Продуктовая линейка построена как путь развития: **Start → Expert → E-passport → Zero Trust.** Каждый следующий уровень добавляет более зрелые сценарии защиты доступа.

Базовые характеристики

Тип продукта
Облачное решение управления безопасным доступом и аутентификацией.

Основной сценарий
MFA, SSO, контроль доступа, защита сессий и устройств.

Модель использования
Cloud / SaaS.

Основные пользователи
Сотрудники, подрядчики, администраторы, внешние пользователи.

Объекты защиты
Web-приложения, VPN, корпоративные порталы, desktop-приложения, legacy-системы, инфраструктурные сервисы.

Основные технологии
MFA, SSO, Access Bridge, E-passport*, Unified SSO, Device Control, Zero Trust*.

Интеграции
OpenID Connect, SAML, RADIUS, LDAP Proxy, Enterprise SSO, Reverse Proxy, Windows Logon, Linux Logon, ADFS, Keycloak.

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Тарифы
Start, Expert, E-passport, Zero Trust.

Цель
Снижение риска компрометации учетных записей, защита доступа и развитие Zero Trust-модели.

Доступная функциональность

Многофакторная аутентификация

MFA позволяет усилить вход в корпоративные системы дополнительными факторами подтверждения.

Поддерживаемые и планируемые сценарии могут включать:

- программный TOTP;
- Push в мобильный аутентификатор;
- усиленный TOTP в мобильном аутентификаторе;
- аппаратный TOTP;
- аппаратные OTP-токены;
- OTP на e-mail;
- резервные способы входа;
- push в мессенджеры;
- SMS-сценарии через собственный или внешний шлюз.

Для чего подходит:

- защита VPN;
- защита web-приложений;
- защита корпоративных порталов;
- усиление входа для сотрудников и подрядчиков;
- выполнение базовых требований ИБ и аудита;
- снижение риска входа по украденному паролю.

SSO для web-приложений

SSO позволяет пользователю один раз пройти аутентификацию и получать доступ к нескольким web-приложениям без постоянного повторного ввода учетных данных.

Для чего подходит:

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- снижение количества паролей;
- упрощение пользовательского опыта;
- уменьшение нагрузки на поддержку;
- централизация доступа к web-приложениям;
- повышение контроля над входом в корпоративные сервисы.

Контекстная и адаптивная аутентификация

Контекстная аутентификация позволяет учитывать обстоятельства входа и применять разные требования к разным сценариям.

Может учитываться:

- IP-адрес;
- группа пользователя;
- атрибуты пользователя;
- тип учетной записи;
- сценарий входа;
- устройство;
- геоконтекст;
- время;
- поведение;
- уровень риска.

Для чего подходит:

- усиление защиты критичных ресурсов;
- более удобный вход для обычных сценариев;
- разные политики для сотрудников, подрядчиков и администраторов;
- снижение риска несанкционированного входа;
- переход от “одинаковой MFA для всех” к риск-ориентированной модели.

Access Bridge

Access Bridge — это компонент, который связывает облачный сервис CURATOR.IDENTITY с реальной инфраструктурой клиента.

Он может разворачиваться:

- в on-prem инфраструктуре;
- в облачной VM;
- в VPS/VDS;
- рядом с приложениями;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- рядом с источниками аутентификации;
- в выделенном сегменте инфраструктуры.

Access Bridge нужен для того, чтобы облачный сервис мог безопасно взаимодействовать с внутренними системами клиента без публикации критичных компонентов наружу.

Для чего подходит:

- подключение LDAP-каталогов;
- интеграция с Microsoft Active Directory, Avanpost DS, OpenLDAP;
- поддержка RADIUS-сценариев;
- защита VPN и сетевого доступа;
- хранение RADIUS/LDAP-секретов в инфраструктуре клиента;
- гибридные сценарии;
- работа с корпоративными протоколами, которые нельзя или неудобно напрямую выносить в интернет.

Ключевая ценность:

Клиент получает преимущества облачной модели, не теряя контроль над внутренней инфраструктурой и секретами.

Reverse Proxy

Reverse Proxy используется для расширенных сценариев защиты приложений через аутентифицирующий прокси.

Для чего подходит:

- защита приложений перед предоставлением доступа;
- добавление аутентификации к существующим сервисам;
- контроль входа в приложения без глубокой модификации самих приложений;
- повышение безопасности web-сценариев.

Windows / Linux Logon

Функциональность logon-сценариев позволяет усиливать вход на рабочие станции и серверы.

Для чего подходит:

- усиление входа на Windows-рабочие станции;
- усиление входа на Linux-системы;
- защита административного доступа;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- снижение риска входа по скомпрометированному паролю;
- применение MFA к инфраструктурным сценариям.

Unified SSO

Unified SSO — это единая защищенная сессия между приложениями, протоколами и точками входа.

В отличие от базового web SSO, Unified SSO ориентирован на более сложную корпоративную среду, где есть не только web-приложения, но и desktop-, legacy-, инфраструктурные и кросс-протокольные сценарии.

Для чего подходит:

- единый вход в web-, desktop-, infrastructure- и legacy-системы;
- снижение повторных вводов пароля;
- повышение удобства пользователей;
- уменьшение нагрузки на поддержку;
- защита сессии в течение рабочего дня;
- централизованное завершение доступа.

E-passport

E-passport — это цифровой идентификатор устройства, реализованный через криптографическую пару ключей. Он помогает подтвердить, что доступ выполняется именно с доверенного устройства, а не с его подмены.

E-passport может использоваться для:

- криптографической привязки доступа к устройству;
- снижения риска перехвата сессии;
- защиты от повторного использования сессии;
- усиления доверия к устройству;
- реализации зрелых сценариев защищенного доступа.

Ключевая идея:

E-passport усиливает не только момент входа, но и доверие к самой сессии и устройству.

Device Control

Device Control позволяет учитывать устройство как полноценный фактор принятия решения о доступе.

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Функциональность может включать:

- инвентаризацию устройств;
- профилирование устройств;
- идентификацию устройства;
- сбор сигналов безопасности;
- анализ состояния устройства;
- использование устройства в логике аутентификации;
- политики доверия;
- отчеты по устройствам и их характеристикам.

Для чего подходит:

- работа с BYOD;
- контроль удаленных сотрудников;
- контроль подрядчиков;
- снижение риска входа с небезопасных устройств;
- реализация Zero Trust-подхода;
- постоянный пересчет доверия к устройству.

Zero Trust

Zero Trust — это модель безопасности, в которой доверие не выдается один раз и навсегда.

Каждый доступ должен проверяться с учетом:

- пользователя;
- устройства;
- контекста;
- уровня риска;
- состояния сессии;
- текущего сценария работы.

В тарифной логике CURATOR.IDENTITY Zero Trust — это наиболее зрелый уровень развития решения, где компания контролирует не только сам вход, но и дальнейшие условия доступа в ходе работы пользователя.

Для чего подходит:

- зрелые ИБ-команды;
- организации с высокой ценой инцидента;
- критичные бизнес-процессы;
- удаленная и гибридная работа;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- подрядчики и внешние пользователи;
- BYOD;
- компании, находящиеся в зоне повышенного интереса злоумышленников.

Тарифная логика

Start

Start — базовая облачная защита доступа для web-приложений, VPN и типовых корпоративных сценариев входа. Тариф подходит компаниям, которым нужно быстро уйти от одной только парольной защиты, включить второй фактор и закрыть базовые требования к защите доступа.

Что помогает сделать Start:

- быстро включить MFA;
- защитить VPN и web-приложения;
- подключить типовые корпоративные сервисы;
- снизить риск входа по украденному паролю;
- выполнить базовые требования ИБ, аудита и регуляторики;
- запустить защищенный доступ без капитальных затрат;
- начать путь к Zero Trust без смены платформы.

Типовые сценарии:

- MFA для VPN;
- MFA для web-приложений;
- SSO для web-приложений;
- интеграция по OpenID Connect, SAML, RADIUS;
- подключение LDAP-каталогов;
- базовые сценарии входа для Linux-систем;
- самостоятельная привязка аутентификатора пользователем.

Expert

Expert — профессиональная многофакторная аутентификация для доступа к сервисам и инфраструктуре на основе контекста и риска. Тариф нужен компаниям, которым уже недостаточно одинаковой MFA для всех пользователей и всех сценариев.

Что помогает сделать Expert:

- задавать разные правила входа для разных групп пользователей;
- усиливать доступ к критичным системам;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- учитывать контекст входа;
- безопаснее работать с подрядчиками и администраторами;
- применять многошаговые MFA-сценарии;
- видеть риски пользователей;
- использовать резервные и аварийные сценарии входа;
- защищать более сложные корпоративные сценарии.

Типовые сценарии:

- разные MFA-политики для сотрудников, подрядчиков и администраторов;
- контекстные правила;
- учет IP-адреса;
- учет атрибутов пользователя;
- расширенные сценарии восстановления;
- Reverse Proxy;
- Windows / Linux Logon;
- риск-ориентированная защита.

E-passport

E-passport — тариф для зрелых сценариев защищенного доступа, где важны Unified SSO, криптографическая защита сессии, аппаратные факторы и защита от перехвата сессии. E-passport нужен организациям, которым уже недостаточно SSO только для web-приложений и обычной MFA.

Что помогает сделать E-passport:

- объединить web-, desktop-, infrastructure- и legacy-доступ;
- снизить количество повторных вводов паролей;
- повысить удобство пользователей;
- защитить пользовательскую сессию;
- снизить риск перехвата и повторного использования сессии;
- использовать аппаратные токены, смарт-карты и электронную подпись;
- применять криптографическую привязку доступа к устройству;
- централизованно управлять сессией.

Типовые сценарии:

- Unified SSO;
- Desktop SSO;
- Enterprise SSO;
- кросс-протокольный SSO;
- защита сессии;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- работа с legacy-системами;
- LDAP Proxy;
- ADFS-интеграции;
- аппаратные аутентификаторы.

Zero Trust

Zero Trust — наиболее зрелый уровень защиты доступа, где доверие к пользователю и устройству непрерывно пересчитывается на основе контекста, состояния и риска. Тариф подходит организациям, которым важно контролировать не только сам вход, но и дальнейшие условия доступа в ходе работы пользователя.

Что помогает сделать Zero Trust:

- принимать решения о доступе с учетом пользователя, устройства, контекста и риска;
- безопасно работать с удаленными сотрудниками, подрядчиками и BYOD;
- контролировать состояние устройств;
- ограничивать доступ при изменении контекста;
- снижать риск развития атаки после успешного входа;
- выстраивать непрерывный контроль доверия;
- получать отчеты по устройствам и подозрительной активности.

Типовые сценарии:

- Device Control;
- инвентаризация устройств;
- профилирование устройств;
- сбор сигналов безопасности;
- анализ состояния устройства;
- политики доверия;
- усиление проверки при смене контекста;
- риск-ориентированные решения о доступе;
- контроль BYOD.

Пользовательский сценарий работы

Конкретный набор шагов может отличаться в зависимости от тарифа, инфраструктуры клиента, выбранных протоколов и требуемого уровня защиты.

Регистрация в облачном личном кабинете

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Администратор создает организацию в облачном кабинете и получает доступ к управлению сервисом.

Подключение Access Bridge

В инфраструктуре клиента разворачивается Access Bridge — компонент, который безопасно связывает облачную платформу с внутренними ресурсами компании. Access Bridge может быть установлен рядом с приложениями, каталогами или источниками аутентификации.

Подключение пользователей и каталогов

Администратор подключает пользователей, группы, корпоративные каталоги и источники учетных данных.

На этом этапе могут использоваться интеграции с Microsoft Active Directory, Avanpost DS, OpenLDAP и другими LDAP-совместимыми каталогами.

Интеграция с защищаемыми системами

Подключаются приложения и сервисы, для которых нужно включить защищенный доступ:

- web-приложения;
- VPN;
- корпоративные порталы;
- инфраструктурные сервисы;
- desktop-приложения;
- legacy-системы;
- сервисы доступа.

Выбор и активация тарифа

Администратор выбирает подходящий тарифный план в зависимости от нужного уровня защиты:

- Start;
- Expert;
- E-passport;
- Zero Trust.

Настройка правил доступа

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Настраиваются сценарии входа, политики MFA, правила SSO, контекстные условия, резервные сценарии и требования к группам пользователей.

Тестирование

Перед переводом в эксплуатацию проводится проверка:

- работает ли вход;
- корректно ли срабатывают факторы;
- доступны ли приложения;
- правильно ли применяются политики;
- есть ли резервные сценарии;
- корректно ли работает Access Bridge.

Запуск в эксплуатацию

После тестирования система переводится в рабочий режим.

Пользователи начинают проходить защищенный вход, а администраторы получают централизованный контроль доступа.

Развитие сценариев

По мере роста требований компания может переходить к более зрелым сценариям:

- расширенные MFA-политики;
- контекстная аутентификация;
- Unified SSO;
- защита сессий;
- контроль устройств;
- Zero Trust.

Правила безопасного использования

CURATOR.IDENTITY должен внедряться с учетом внутренних регламентов клиента, критичности систем и требований безопасности.

Важно:

- не отключать резервные сценарии без согласования;
- заранее тестировать политики на пилотных группах;
- не применять строгие политики сразу ко всем пользователям без проверки;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

- отдельно тестировать доступ администраторов;
- предусматривать emergency access;
- документировать изменения политик;
- учитывать влияние на бизнес-процессы;
- проверять работу Access Bridge;
- согласовывать MFA-сценарии с ИТ и ИБ;
- обучать пользователей первому входу и self-service сценариям.

Отличие от обычного MFA-сервиса

Обычный MFA-сервис добавляет второй фактор к входу.

CURATOR.IDENTITY решает более широкую задачу:

- управляет разными сценариями доступа;
- поддерживает SSO;
- учитывает контекст входа;
- позволяет развивать защиту по тарифным уровням;
- поддерживает гибридную инфраструктуру через Access Bridge;
- защищает не только вход, но и сессию;
- работает с web-, desktop-, legacy- и infrastructure-сценариями;
- позволяет двигаться к Zero Trust.

Отличие от SSO

SSO делает вход удобнее: пользователь один раз проходит аутентификацию и получает доступ к нескольким приложениям.

CURATOR.IDENTITY использует SSO как часть более широкой модели защищенного доступа.

Помимо SSO, продукт может включать:

- MFA;
- контекстные политики;
- риск-ориентированную аутентификацию;
- Access Bridge;
- Reverse Proxy;
- E-passport;
- защиту сессии;
- контроль устройств;
- Zero Trust-сценарии.

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Отличие от PAM

PAM фокусируется на управлении привилегированным доступом: администраторами, суперпользователями, критичными учетными записями и сессиями с повышенными правами.

CURATOR.IDENTITY фокусируется шире — на защищенном доступе сотрудников, подрядчиков и пользователей к корпоративным системам.

Решение может усиливать доступ администраторов и привилегированных пользователей, но не должно автоматически позиционироваться как полноценная замена PAM без отдельного подтверждения функциональности.

Отличие от MDM / EDR

MDM управляет устройствами: настройками, политиками, приложениями, конфигурациями и ограничениями.

EDR выявляет и расследует угрозы на endpoint-устройствах.

CURATOR.IDENTITY не заменяет MDM или EDR. Но в зрелых сценариях он может учитывать устройство при принятии решения о доступе.

Отличие от Zero Trust Network Access

ZTNA обычно контролирует доступ к приложениям и сетевым ресурсам по принципу Zero Trust.

CURATOR.IDENTITY реализует Zero Trust-подход через идентичность, аутентификацию, сессии, устройство, контекст и риск.

FAQ

Нужно ли устанавливать агент?

Для базовых cloud-сценариев может быть достаточно облачной платформы и интеграций. Для гибридных сценариев, подключения внутренних каталогов, RADIUS/LDAP и взаимодействия с инфраструктурой клиента используется Access Bridge.

Что такое Access Bridge?

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Access Bridge — это компонент, который разворачивается рядом с инфраструктурой клиента и безопасно связывает внутренние системы с облачным сервисом CURATOR.IDENTITY.

Он позволяет работать с корпоративными каталогами, RADIUS-, LDAP- и другими сценариями без публикации внутренних сервисов наружу.

Можно ли начать только с MFA?

Да. Для этого подходит тариф Start. Он позволяет быстро уйти от одной только парольной защиты и включить второй фактор для типовых корпоративных сценариев.

Чем Expert отличается от Start?

Start закрывает базовую защиту входа. Expert добавляет более гибкие и интеллектуальные сценарии: разные политики для групп пользователей, контекст входа, многошаговые MFA-сценарии, риск-ориентированную защиту и расширенные возможности для критичных систем.

Чем E-passport отличается от Expert?

Expert усиливает MFA и контекстную аутентификацию. E-passport добавляет более зрелые сценарии Unified SSO, desktop- и legacy-доступа, криптографическую защиту сессии и привязку доступа к доверенному устройству.

Что такое E-passport?

E-passport — это цифровой идентификатор устройства, основанный на криптографической паре ключей. Он помогает подтвердить, что доступ выполняется именно с доверенного устройства, а не с подмененного или неизвестного endpoint.

Что такое Unified SSO?

Unified SSO — это единая защищенная сессия между разными приложениями, протоколами и точками входа. Это более зрелый сценарий, чем обычный web SSO, потому что он может охватывать desktop-, legacy- и инфраструктурные системы.

Что такое Zero Trust в контексте решения?

Zero Trust — это подход, при котором доступ проверяется не один раз, а постоянно: по пользователю, устройству, контексту и риску. В CURATOR.IDENTITY эта логика развивается через MFA, SSO, E-passport, Device Control и непрерывный контроль доверия.

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

Может ли решение заменить пароли полностью?

Не всегда. В большинстве сценариев решение усиливает и контролирует вход, добавляет MFA, SSO и другие механизмы. Возможность passwordless-сценариев зависит от конкретной реализации, тарифа и инфраструктуры клиента.

Подходит ли решение для подрядчиков?

Да. Один из важных сценариев — безопасный доступ подрядчиков и внешних пользователей к корпоративным системам с отдельными правилами, ограничениями и повышенным контролем.

Подходит ли решение для BYOD?

Да, особенно в зрелых сценариях с Device Control и Zero Trust. Решение помогает учитывать устройство при принятии решения о доступе, но не заменяет полноценную MDM-стратегию.

Можно ли подключить VPN?

Да. Для VPN и сетевого доступа используются RADIUS-сценарии и соответствующие интеграции.

Поддерживаются ли web-приложения?

Да. Для web-приложений могут использоваться OpenID Connect, SAML, SSO и другие сценарии интеграции.

Поддерживаются ли legacy-приложения?

На старших тарифах продуктовая логика предусматривает поддержку более зрелых сценариев, включая Enterprise SSO, LDAP Proxy, desktop- и legacy-доступ.

Что делать после базового внедрения?

Рекомендуется постепенно развивать модель:

1. включить MFA;
2. подключить основные приложения;
3. настроить SSO;
4. разделить пользователей по группам;
5. усилить доступ к критичным системам;
6. добавить контекстные политики;

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.

7. подключить Unified SSO;
8. внедрить E-passport;
9. добавить контроль устройств;
10. перейти к Zero Trust-сценариям.

***** Решения Zero Trust и E-passport находятся в разработке и запланированы к запуску в 4 квартале 2026 года.