Curator.Identity sales guide

О решении

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

Решение позволяет компаниям быстро запускать MFA и SSO, усиливать контроль устройств и пользовательских сессий, а также постепенно выстраивать архитектуру защищенного доступа — от базовой многофакторной аутентификации до зрелых Zero Trust-сценариев.

Curator.Identity помогает защищать доступ к web-приложениям, VPN, корпоративным порталам, инфраструктурным сервисам, desktop- и legacy-приложениям. Решение снижает риск компрометации учетных записей, перехвата сессий и несанкционированного входа в критичные системы.

Какую задачу решает

Современные атаки все чаще начинаются не с классического взлома внешнего периметра, а с компрометации учетных записей.

Злоумышленники получают доступ к инфраструктуре под видом легитимных пользователей: используют украденные логины и пароли, слабые MFA-сценарии, скомпрометированные токены, cookie, активные сессии и внешние сервисы доступа.

Для бизнеса это означает, что даже при наличии сетевой защиты, WAF, мониторинга и других инструментов безопасности остается критический риск: злоумышленник может войти в корпоративную систему как обычный сотрудник, подрядчик или администратор.

Curator.Identity помогает закрыть этот риск за счет централизованного управления доступом, усиленной аутентификации, SSO, контроля сессий, учета контекста и постепенного перехода к Zero Trust.

Основные задачи:

- уход от одной только парольной защиты;
- снижение риска компрометации учетных записей;
- защита удаленного доступа сотрудников и подрядчиков;
- усиление входа в VPN, web-приложения и корпоративные порталы;

- внедрение SSO без тяжелого on-prem проекта;
- контроль контекста входа: пользователь, группа, IP-адрес, устройство, сценарий доступа;
- снижение риска перехвата и повторного использования пользовательской сессии;
- защита доступа к legacy-, desktop- и инфраструктурным приложениям;
- постепенный переход к Zero Trust-модели;
- снижение нагрузки на ИТ и службу поддержки за счет self-service сценариев и единого входа.

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.

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.

Как объяснять продукт клиенту

Простое объяснение

Curator.Identity помогает компании контролировать, кто и на каких условиях получает доступ к корпоративным системам. Это не просто второй фактор. Это решение, которое объединяет MFA, SSO, контроль сессий, контекст доступа и устройства.

Объяснение для бизнеса

Решение снижает риск простоев, утечек и инцидентов, которые начинаются с украденных учетных данных или перехваченных сессий. При этом он не усложняет работу сотрудников, а помогает сделать вход удобнее через SSO и self-service сценарии.

Объяснение для ИТ

Решение позволяет централизованно управлять аутентификацией, подключать приложения и инфраструктуру через стандартные протоколы, снижать количество ручных операций и постепенно развивать политику доступа.

Объяснение для ИБ

Curator.Identity помогает перейти от формальной MFA к риск-ориентированному доступу: учитывать пользователя, группу, устройство, IP-адрес, контекст, сессию и уровень риска.

Рекомендации для старта продаж

Когда предлагать Start

Предлагать, если клиент:

- до сих пор использует только пароли;
- хочет быстро включить MFA;
- защищает VPN и web-приложения;
- готовится к аудиту;
- хочет быстрый старт без сложного внедрения;
- пока не готов к сложным Zero Trust-сценариям.

Когда предлагать Expert

Предлагать, если клиент:

- уже понимает ограничения базовой MFA;
- хочет разные политики для разных групп;
- имеет подрядчиков и удаленных сотрудников;
- защищает критичные системы;
- хочет учитывать контекст входа;

- хочет снизить риск несанкционированного доступа.

Когда предлагать E-passport

Предлагать, если клиент:

- имеет много приложений и точек входа;
- хочет снизить количество повторных вводов пароля;
- использует desktop- и legacy-системы;
- хочет защитить сессию;
- хочет повысить удобство и безопасность одновременно;
- опасается перехвата сессий.

Когда предлагать Zero Trust

Предлагать, если клиент:

- зрелый с точки зрения ИБ;
- имеет высокую цену инцидента;
- работает с BYOD;
- активно использует подрядчиков;
- хочет контролировать устройства;
- хочет постоянно пересчитывать доверие;
- последовательно внедряет Zero Trust-архитектуру.

Основные возражения и ответы

У нас уже есть MFA

Наличие MFA — это хороший первый шаг, но не всегда достаточный. Важно понять, насколько MFA устойчива к современным атакам, учитывает ли она контекст, позволяет ли работать с разными группами пользователей и защищает ли сессию после входа.

Curator.Identity позволяет развивать MFA до полноценной модели защищенного доступа.

Нам достаточно SSO

SSO решает задачу удобства, но не всегда решает задачу безопасности. Если SSO не дополняется MFA, контекстом, контролем сессии и устройствами, он может стать единой точкой риска.

Curator.Identity объединяет удобство SSO с механизмами защиты доступа.

Облако для доступа — это риск

Curator.Identity использует гибридную архитектуру с Access Bridge. Внутренние каталоги, сервисные учетные записи и секреты не требуют публикации наружу и могут оставаться в контролируемом контуре клиента.

Пользователи будут сопротивляться

Продукт учитывает удобство пользователей: SSO, self-service, привязка аутентификатора при входе, снижение повторных вводов пароля и гибкие политики помогают снизить сопротивление.

Нам нужен Zero Trust, но это слишком сложно

Zero Trust не обязательно внедрять сразу целиком. Curator.Identity позволяет двигаться поэтапно: Start → Expert → E-passport → Zero Trust

У нас много legacy-систем

Для этого предусмотрены старшие сценарии: Enterprise SSO, LDAP Proxy, desktop SSO, Unified SSO и Access Bridge.

Что будет, если облако недоступно?

Для гибридных сценариев используется Access Bridge и резервные сценарии аутентификации. Конкретная модель отказоустойчивости зависит от тарифа, архитектуры клиента и настроек.