IBM Security

Модернизация стратегии CIAM в масштабе всей организации общими усилиями всех заинтересованных сторон

IBM

Знакомство

Введение

Когда вы регистрируете новую учетную запись, совершаете покупку или даже просто подписываетесь на новостную рассылку, вы доверяете организации свою персональную информацию. Предоставив эту информацию, вы вряд ли захотите, чтобы она использовалась не только для оговоренных целей. Но, возможно, вы не откажетесь от персонализированного взаимодействия и получения рекомендаций на будущее. Главное, чтобы это зависело исключительно от вас, и вы в любой момент могли изменить свое решение. Но если в процессе вашего взаимодействия с организацией возникнут какие-либо недоразумения, или по какой-либо причине вы перестанете ей доверять, скорее всего, вы прекратите работать с этой организацией и найдете другую. Управление идентификационными данными и доступом потребителей (CIAM) позволяет установить доверительные, адаптивные и персонализированные отношения между потребителем и брендом. Планируя модернизацию цифровых стратегий своей компании для сохранения конкурентоспособности, вы сможете лучше понять проблемы своих клиентов.

Но CIAM — это намного больше, чем просто очередное обновление веб-сайта или маркетинговый проект: эта стратегия предполагает оценку и модернизацию точек взаимодействия с клиентами, а это уже затрагивает все функциональные подразделения организации. Ради сохранения оптимального баланса между удобством и безопасностью все заинтересованные лица в области технологий и бизнеса должны объединить усилия, чтобы система CIAM не только встала на те же технологические рельсы, что и IAM для сотрудников компании, но и превратилась в неотъемлемую составляющую цифровой трансформации, ориентированную на результат. Стратегическое и целенаправленное внедрение этой системы поможет организациям максимально тесно взаимодействовать с потребителями, практически не подвергая риску специалистов по ИТ и безопасности.

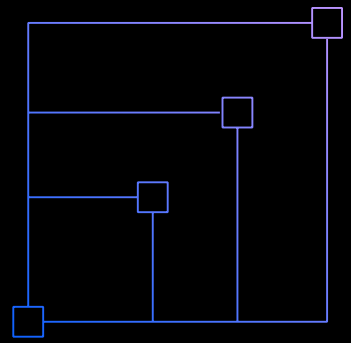
Без хорошей стратегии CIAM предприятия рискуют потерять прибыль из-за ухода клиентов: когда рынок перенасыщен, лояльность к бренду становится довольно хрупкой вещью. Аналогия прослеживается и в государственном секторе: учреждения, которые до сих пор не в силах отказаться от устаревших инфраструктур и устаревших процессов, могут потерять авторитет среди граждан и оказаться неспособными качественно оказывать государственные услуги. Хотя задачи у коммерческого и государственного секторов разные, цель у них, по сути, одна: безупречное и вместе с тем безопасное обслуживание клиентов и обмен информацией со строгим соблюдением конфиденциальности. Об этом задумывается все больше организаций, поэтому направление CIAM уже составляет самую большую часть общего рынка IAM и, по прогнозам, до 2025 года его доля будет ежегодно расти на 15,1%[1]. Для тех, кто еще не приступил к цифровой модернизации, одним из первоочередных и важнейших шагов должно стать согласование действий руководства различных функциональных подразделений: только это сделает проект выгодным для всех сторон.

Директора по маркетингу (CMO)

Цель CIAM: привлечение, подготовка и развитие клиентов за счет персонализированного взаимодействия, которое контролируется пользователем и не нарушает его конфиденциальность.

В коммерческом секторе маркетологи усиленно борются за внимание потенциальных клиентов, и последнее, чего бы они хотели, — это сложности при регистрации, которые могут оттолкнуть клиентов в последний момент. Уход клиентов может напрямую влиять на прибыль. Программы CIAM помогают предотвратить его, упрощая регистрацию и начальное взаимодействие клиента с брендом. Это позволяет превратить абстрактных потенциальных клиентов в реальные и перспективные бизнес-возможности. В идеале формы регистрации новых клиентов должны запрашивать как можно меньше информации, а точки взаимодействия должны быть настроены таким образом, чтобы по мере развития взаимоотношений с этим клиентом организации могли узнавать о нем больше и больше.

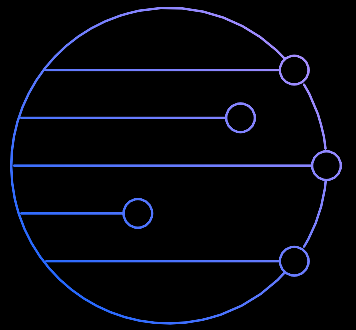
В крупных организациях со множеством дочерних брендов хранилища данных должны проектироваться так, чтобы собирать и вести один профайл для каждого клиента. Они должны интегрироваться с системами управления взаимоотношениями с клиентами (CRM) и другими сторонними инструментами и системами. При централизованном управлении идентификационными данными клиентов стратегическое внедрение современных технологий CIAM поможет маркетологам лучше понимать поведение их клиентов и проводить более персонализированные рекламные кампании, точно подобранные под целевую аудиторию. CIAM играет главную роль в цифровом взаимодействии как с новыми, так и со старыми клиентами, поэтому руководители отделов маркетинга естественным образом становятся центральным звеном процесса планирования модернизации.



Руководители производственных подразделений

Цель CIAM: обеспечить рациональное и удобное взаимодействие с помощью современных интерфейсов и инструментов для достижения целей организации

Руководители предприятий или владельцы агентств точно так же заинтересованы в привлечении клиентов и удобном взаимодействии с ними, хотя прибыль от этого напрямую и не зависит. Например, от государственных учреждений, в которых обычно нет специализированного маркетингового отдела, требуется эффективное предоставление населению государственных услуг и модернизация способов взаимодействия с гражданами с учетом их разнообразных предпочтений и каналов связи. Владельцы агентств тоже стремятся перестроить общение с пользователями: упрощая регистрацию, они снижают вероятность ухода пользователя и повышают качество оказания услуг. Хотя эти организации и не проводят никаких рекламных кампаний, они все равно стремятся вести единый профайл каждого клиента: это позволяет упростить взаимодействие клиентов с разными подразделениями, исключить двойную работу и лучше понять поведение пользователей.



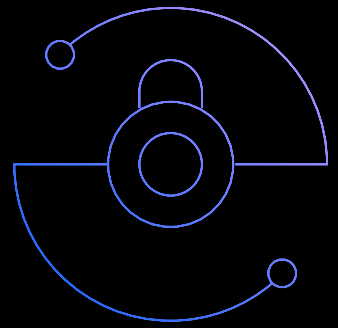
Директора по безопасности и конфиденциаль-ности

Цель CIAM: обеспечить безопасное и прозрачное взаимодействие с клиентами для соблюдения нормативных требований, передачи контроля пользователю, а также предотвращения мошенничества и компрометации учетных записей

Основной принцип — потребители должны знать, кто контролирует их данные и как они используются, а также иметь возможность самостоятельно управлять своими данными и в любое время изменять решение о согласии на их передачу. Уже одно это — достаточная причина, чтобы поставить управление конфиденциальностью и согласием во главу угла цифрового взаимодействия, но еще большую остроту этому вопросу придают мировые законы. Предприятия обязаны соблюдать правила в каждом регионе, в котором они ведут свою деятельность, иначе им грозят внушительные штрафы и пени. Но, хотя законы о конфиденциальности подробно регламентируют действия организаций, они обычно не содержат никаких инструкций о том, как этого добиться.

Грамотно реализованная система CIAM выступает в качестве единого источника достоверной информации в отношении всей персональной информации (PII). Директора по конфиденциальности и нормативному соответствию могут определять правила и политики для разных задач, связанных с управлением согласием — тогда техническим специалистам остается просто применять эти политики для необходимых приложений. Такой подход позволяет специалистам по конфиденциальности и нормативному контролю выйти за рамки электронных таблиц, в полной мере адаптироваться к стремительно меняющимся законам о конфиденциальности и упростить их соблюдение.

Хотя директора по ИТ-безопасности (CISO) не меньше руководителей отделов нормативного контроля заинтересованы в обеспечении конфиденциальности и управлении согласием, возможны варианты, когда CISO рассматривают CIAM как маркетинговый проект и теряют к нему интерес ради более приоритетных задач. Несмотря на то, что цели и перспективы традиционных систем IAM для сотрудников и для потребителей действительно совершенно разные, все же



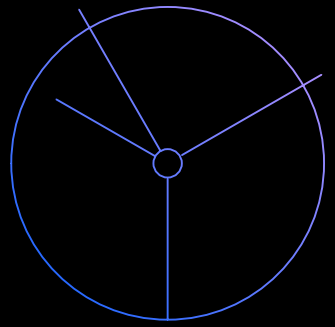
коммерческие решения с их безопасным хранением данных и снижением риска утечек пойдут на пользу обеим сторонам: идентификационные данные клиентов не меньше нуждаются в защите, чем идентификационные данные сотрудников. К тому же, если реализовывать проекты CIAM без стратегического анализа текущего состояния инфраструктуры IAM, то в конечном счете может оказаться, что в среде организации прибавилось множество разрозненных фрагментов решений, которые только увеличивают риск за счет дополнительных точек доступа. Поэтому именно в интересах CISO по возможности объединить системы управления идентификационными данными и доступом сотрудников и потребителей в единое решение, позволяющее избежать ненужного разобщения данных.

ИТ-директора (CIO)

Цель CIAM: снизить сложность внедрения и сопровождения решений IAM, обеспечить соответствие новейшим стандартам в отношении управления идентификацией и современным требованиям к безопасности

Если отступить от преимуществ CIAM в плане привлечения клиентов, то ИТ-директор должен уметь оценить, впишется ли каждое новое технологическое решение в уже сложившуюся инфраструктуру и в планы организации. Перспектива упрощения и стандартизации всегда работает безотказно, поэтому интеграция функций IAM и CIAM в едином инструменте должна найти отклик не только у специалистов по безопасности, но и у ИТ-руководства. Такой подход поможет избежать не только лишнего усложнения ИТ-среды в целом, но и избавить организацию от необходимости обучения имеющихся сотрудников новым навыкам. Также велика вероятность, что использование одного решения для управления идентификацией и внутренних, и внешних групп пользователей будет выгодным с точки зрения затрат, сводя к минимуму текущие ИТ-расходы.

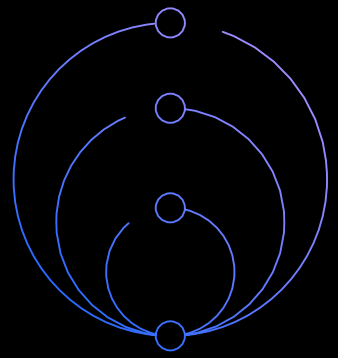
Как только решение CIAM начнет работать в полную силу, каждая минута простоя может обернуться губительной потерей времени и прибыли для организаций, клиенты которых не смогут получить доступ к своим учетным записям. Уже одно это объясняет, почему многие ИТ-руководители предпочитают облачные решения для CIAM: как правило, они намного быстрее окупаются, обеспечивая более высокую доступность и масштабируемость по сравнению с локальными альтернативами. К тому же, облачная система IAM имеет и ряд других преимуществ: не нужно обслуживать ИТ-инфраструктуру, программное обеспечение обновляется автоматически, а ввод решения в эксплуатацию происходит намного быстрее.



Администраторы и разработчики IAM

Цель CIAM: облегчение жизни разработчиков, защита и сопровождение политик для приложений с помощью малокодовых процессов, основанных на конфигурации

Пока руководители высшего звена на своем уровне согласовывают бизнес-цели, операционные затраты и снижение рисков, администраторы и разработчики IAM могут влиять на развитие программы CIAM, всесторонне оценивая технические возможности решений. В частности, они будут анализировать логистику миграции или объединения источников данных и приложений, а также такие немаловажные аспекты, как поддерживаемые протоколы аутентификации, методы мультифакторной идентификации и каналы доставки. Если говорить об ускорении ввода в эксплуатацию, то здесь можно оценить документацию по API решений, наличие и качество справочных руководств, обучающих материалов и инструментария малокодового программирования. Не менее важна также уверенность ИТ-специалистов в надлежащей поддержке со стороны руководства на этапах внедрения и сопровождения решения. Функции CIAM, в основе которых лежат рабочие процессы (например, управление согласием), могут сберечь нервы разработчиков, например, благодаря сведению пунктов законов о конфиденциальности к простым обращениям к API, автоматически учитывающим изменения требований. Прежде чем добавлять в комплекс очередной инструмент, технические специалисты должны всесторонне оценить его совместимость и интеграцию с уже имеющимися решениями IAM, и понять, насколько слаженно будет работать система в долгосрочной перспективе.



Интегрированный подход IBM к CIAM

Модернизация цифрового опыта с помощью интегрированного подхода IBM к CIAM

Решения и услуги IBM Security помогут вашей организации привлекать клиентов и налаживать адаптивные и персонализированные взаимоотношения с ними по любому каналу взаимодействия. Этому способствует продуманный комплекс, состоящий из стратегий идентификации, отлаженных методов цифрового проектирования и облачных технологий CIAM. Использование IBM Security Verify в комбинации с услугами IBM Security помогает обеспечить согласованность действий в масштабах всей организации, деликатное и вместе с тем точное отслеживание информации о потребителях, а также предоставление им простого и безопасного способа цифрового взаимодействия с вашим брендом.

Следующие шаги

Подробнее о CIAM
Лучшие наработки, советы по планированию и подводные камни систем CIAM

Загрузить руководство →

Обзор IBM Security Verify
Использование IDaaS для модернизации взаимодействия с пользователями посредством входа в систему через социальные сети и адаптивной идентификации, а также соблюдение конфиденциальности за счет управления согласием

Подробнее о Verify →

Услуги IBM Security для CIAM
Уникальный подход на основе консультирования и сотрудничества к планированию, проектированию и реализации программы CIAM в соответствии с бизнес-целями организации

Получить помощь для CIAM →

IBM EE/A
123112 Москва
Пресненская наб., 10

Произведено в США.
Февраль 2021 г.

Настоящий документ актуален по состоянию на момент публикации и может быть изменен IBM в любое время. Не все предложения могут быть доступны во всех странах, в которых IBM ведет свою деятельность. Приведенные данные о производительности и примеры клиентов служат исключительно для иллюстрации. Фактические результаты могут отличаться в зависимости от конфигурации и условий работы. ИНФОРМАЦИЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ ПРЕДОСТАВЛЯЕТСЯ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ И УСЛОВИЙ, КАК ЯВНЫХ, ТАК И ПОДРАЗУМЕВАЕМЫХ, В ТОМ ЧИСЛЕ БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ ТОВАРОПРИГОДНОСТИ, СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, А ТАКЖЕ КАКОЙ-ЛИБО ГАРАНТИИ ИЛИ УСЛОВИЯ НЕНАРУШЕНИЯ ПРАВ.

Заявление о добросовестной политике безопасности: В процесс обеспечения безопасности ИТ-систем входит защита систем и информации путем предотвращения, обнаружения и блокирования несанкционированного доступа к ним изнутри и снаружи организации. Несанкционированный доступ может привести к подмене, уничтожению, краже или неправомерному использованию информации, повреждению систем или их использованию в корыстных целях, в том числе для осуществления атак на других пользователей. Ни одну ИТ-систему или продукт нельзя считать абсолютно безопасными, равно как ни один продукт, услуга или мера безопасности не может обеспечить абсолютную эффективность в предотвращении несанкционированного доступа или неправомерного использования. Системы, продукты и услуги IBM предназначены для работы в комплексе законных мер по обеспечению безопасности, в который для максимальной эффективности обязательно будут входить другие процедуры и, возможно, будут задействоваться другие системы, продукты и услуги. IBM НЕ ГАРАНТИРУЕТ, ЧТО ЛЮБЫЕ СИСТЕМЫ, ПРОДУКТЫ И УСЛУГИ ПОЛНОСТЬЮ ЗАЩИЩЕНЫ ОТ ЗЛОНАМЕРЕННЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ ЛЮБОЙ ИЗ СТОРОН ИЛИ ЗАЩИТЯТ ВАШЕ ПРЕДПРИЯТИЕ ОТ ПОДОБНЫХ ЗЛОНАМЕРЕННЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ.

[1] Markets and Markets, прогноз мирового рынка IAM для потребителей до 2025 года