okta | auth0

Votre solution CIAM

Trouver la bonne solution de Gestion des accès et des identités clients (CIAM) pour assurer la croissance de votre entreprise

WHITEPAPER

auth0.com

Contenu

Pourquoi vous avez besoin d'une solution CIAM

Vous devez assurer les missions suivantes:

- Favoriser l'inscription des clients
- Vendre aux clients ou supporter des interactions
- Fidéliser vos clients

Et tout doit se faire en toute sécurité et avec transparence. La complexité est liée à l'exécution de la gestion des accès aux clients et aux identités (CIAM).

L'entreprise numérique est désormais un secteur à part entière

L'exécution de votre CIAM joue un rôle crucial.

En fait, **80 % des clients** déclarent que l'expérience offerte est tout aussi importante que le produit. Ils s'attendent à bénéficier d'accès sécurisés, avec maîtrise des données et récupération rapide des comptes en quelques clics. Pour vos clients, ce sont les vrais enjeux.

Mais sans une exécution planifiée et contrôlée, les coûts peuvent largement déraper. Si vous demandez à votre équipe de se concentrer sur l'identité en plus de vos produits de base, vous pourriez gaspiller des énergies et des talents en matière de développement, de sécurité et d'informatique. Une expérience utilisateur entravée peut avoir un impact direct sur la croissance de vos revenus. Et les risques liés à la sécurité, à la conformité et à la fiabilité peuvent susciter de plus grandes inquiétudes. D'après le **DBIR 2021 de Verizon**, 61 % des violations en 2021 impliquaient des informations d'identification compromises.

De plus, l'escalade des réglementations sur la protection des données personnelles, l'interopérabilité et la portabilité des données obligera vos développeurs les plus demandés à se mettre rapidement à niveau dans de nouveaux domaines de pointe.

Comment répondre aux vrais enjeux

Une solution CIAM robuste peut rapidement relever ces défis. Elle permettra à vos talents technologiques de se concentrer sur l'amélioration de votre produit au-delà des attentes, pour répondre aux vrais enjeux. Une solution CIAM puissante ne se contente pas de résoudre le problème du mois ou de l'année. Elle suit le rythme (ou même suggère) des innovations pour votre organisation.

Ce guide vous aidera à définir votre évaluation pour mieux choisir la solution qui convient à votre entreprise aujourd'hui, et dans cinq ans. Vous évaluerez six domaines clés : l'expérience client, l'évolutivité, l'extensibilité, la sécurité, la connaissance du client et les coûts opérationnels.

Expérience client

Vos clients ont-ils confiance en vous?

Vous avez une possibilité très limitée de convertir des clients potentiels en ligne. Avant de prendre une décision, la plupart des utilisateurs ont besoin de percevoir la valeur de la marque. Des frictions nuisent directement à la conversion dès l'enregistrement/la connexion ou si une méfiance peut seulement être perçue à l'égard de la marque.

> «Pour les ingénieurs, rien n'est plus important que l'expérience utilisateur. Tout le travail doit être assuré en coulisses, par le système. Pour le client final, l'expérience utilisateur doit être transparente et aussi simple que possible.»
>
> — DAN LAKE, DIRECTEUR DE L'INGÉNIERIE, GYMSHARK

Avez-vous les outils pour convertir et fidéliser vos clients?

D'après une enquête **PwC**, les clients abandonneraient les marques qu'ils aiment après une seule expérience négative. 70 % des personnes interrogées ont déclaré que « la rapidité, la commodité, un service utile et des employés sympathiques » étaient les facteurs les plus importants: «Les bonnes solutions donnent la priorité aux technologies qui favorisent ou procurent ces avantages, au lieu de seulement être à la pointe du progrès.» Vos efforts dans les domaines suivants seront les plus fructueux:

- **La fondation sans friction:** Toute expérience client numérique réussie commence par un flux personnalisable et sans friction. Ce flux peut inclure des applications intelligentes de bots de chat, des parcours de découverte de produits et des recommandations qui combinent une réflexion attentionnée et des objectifs pratiques, en évitant tout risque de perception négative, intrusif en particulier.
- **La connexion par réseau social est indispensable.** Pour les consommateurs qui sont prêts à faire un achat impulsif ou qui sont simplement devenus prudents (ou lassés) à l'idée d'une autre combinaison nom d'utilisateur/mot de passe, la connexion par réseau social leur offre la rapidité, la facilité et un sentiment de sécurité accru, car les utilisateurs choisissent la quantité d'informations qu'ils partagent.
- **Pouvez-vous évaluer votre impact?** Certaines solutions CIAM présentent des métriques prêtes à l'emploi qui ne mesurent que des données de base. Des options CIAM plus solides incluent des écosystèmes intégrés, qui vous permettent de consommer vos données selon vos besoins. Quelle que soit la façon dont vous souhaitez exploiter vos données clients, et pour réellement comprendre votre entonnoir, vous devez avoir accès à toute la richesse des informations injectées dans vos outils analytiques.

Hesta obtient un Net Promoter Score de 36.2 (2021)

Après la mise en œuvre, 61 % des membres d'HESTA ont déclaré que leur expérience numérique est maintenant « très facile ».

- **En fait, le respect se développe avec le temps et apporte donc ses propres avantages.** Certains clients préfèrent vous donner seulement le minimum d'informations dont vous avez besoin pour exécuter une transaction. Saisissez alors cette opportunité pour développer une relation mutuellement bénéfique, à long terme, basée sur le respect.

Le client constate qu'en partageant plus d'informations, il bénéficie de meilleurs avantages. Vous avez prouvé qu'il pouvait vous confier ses données.

Évolutivité

Si l'expérience client est primordiale, vous avez aussi besoin d'une excellente capacité d'adaptation à des millions d'utilisateurs, voire des milliards, souvent en réponse à des événements de courte durée comme le Black Friday ou la Coupe du monde.

Si votre solution CIAM n'est pas évolutive, elle ne pourra pas fonctionner, puisque votre public cible n'est pas captif. Vos clients disposent même d'un choix particulièrement étendu. Si la commande d'un savoureux sandwich chez vous n'aboutit pas, ils iront immédiatement ailleurs en seul clic pour satisfaire leur faim.

Ce qui explique pourquoi de nombreuses entreprises choisissent un fournisseur tiers fiable plutôt que tenter des résoudre eux-mêmes les challenges de l'évolutivité.

> «L'équilibre entre utilisabilité et sécurité ne nous laisse aucune marge d'erreur. En finalité, nous donnons accès à des données très sensibles, critiques, extrêmement réglementées et qui pourraient avoir des conséquences réelles sur la vie de quelqu'un.»
>
> —LANA COHEN, DIRECTRICE DE LA GESTION DES PRODUITS, ATHENAHEALTH (4 MILLIONS DE PATIENTS SERVIS SUR 8 000 PORTAILS)

Assurez votre pérennité dès maintenant

Comme nous l'avons dit, vous pouvez évaluer une solution CIAM pour résoudre un problème actuel. Mais en réalité, vous devez prévoir où vous voulez être dans cinq ans. Sans cela, vous vous exposez à de sérieuses difficultés, probablement douloureuses, pour atteindre ce futur tant espéré.

Savoir si votre fournisseur peut ou non gérer l'évolutivité requise est une question simple. Voici quelques questions supplémentaires pour votre équipe:

- **Où voyez-vous votre entreprise dans cinq ans?** Quelles sont les implications pour vos besoins en termes d'évolutivité? En réfléchissant de manière stratégique à l'avenir de votre entreprise, vous éviterez de créer par inadvertance des incompatibilités et des écarts technologiques.
- **Avec quelle rapidité pouvez-vous mettre votre produit sur le marché?** Votre solution CIAM n'est pas évolutive si vous mesurez votre progression en années.
- **Quel est votre budget de maintenance courant?** Une maintenance permanente restera nécessaire rien que pour permettre à vos utilisateurs de continuer à se connecter facilement à votre produit. Votre budget de maintenance continue devrait inclure des mises à jour régulières du chiffrement et une stratégie de protection contre les cyberattaques.

> «Je pense que personne n'aurait jamais pu prévoir que les volumes seraient multipliés par 25 du jour au lendemain. Nous avons réellement testé les limites maximales du débit!».
>
> — VINNY PACIONE, VP DES SOLUTIONS NUMÉRIQUES ET DES TECHNOLOGIES CONSOMMATEURS, BIOREFERENCE LABS

La CIAM est bien plus qu'un simple système de connexion

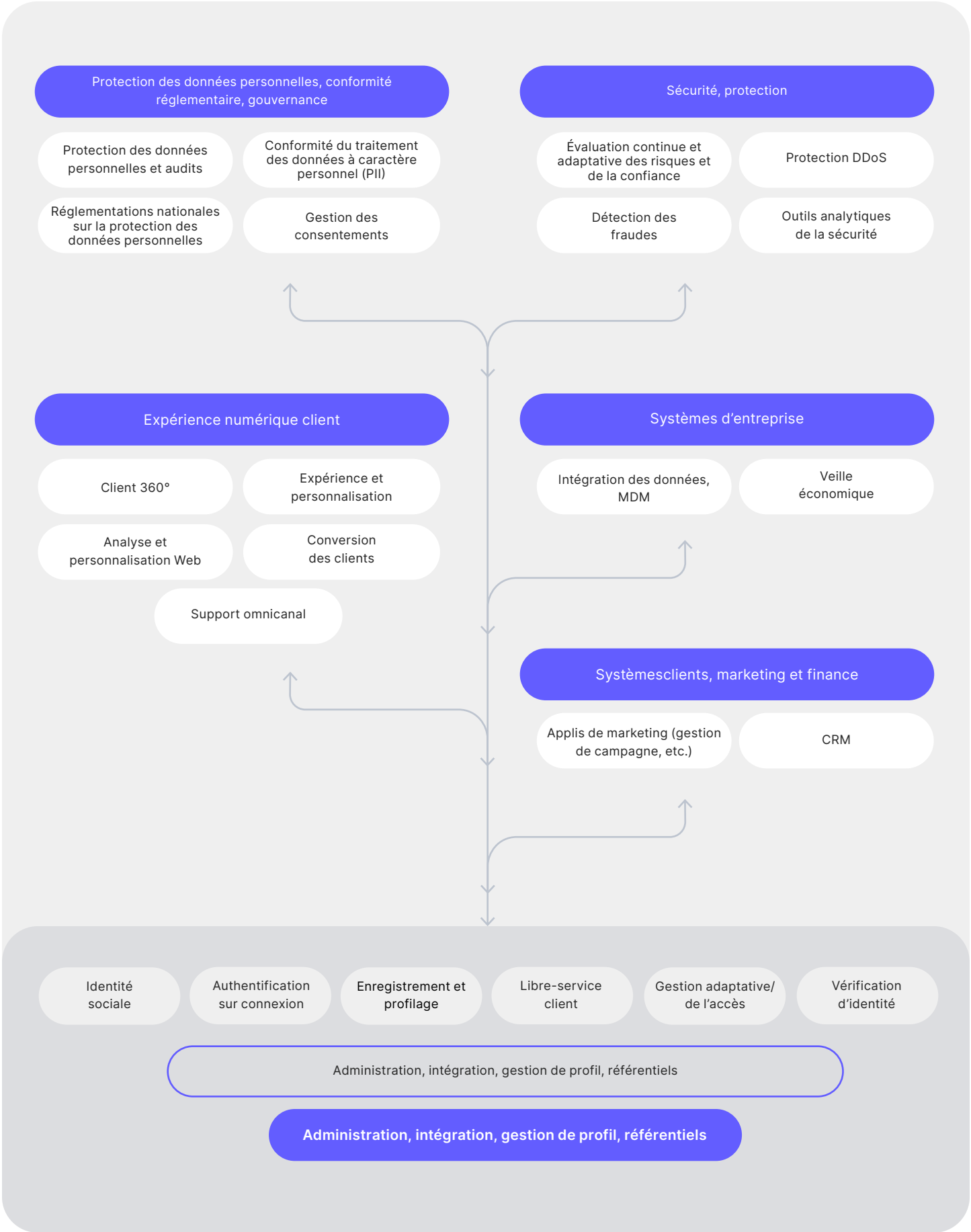
La solution que vous choisirez pour alimenter votre système de connexion réunira un grand nombre de pièces mobiles. Et elles devront évoluer en continu et à long terme pour répondre aux besoins changeants de vos clients, et à leurs demandes, sans parler de votre propre stratégie commerciale. Vous avez donc besoin d'un partenaire capable d'innover en continu. Il vous ouvrira des possibilités commerciales jusqu'alors insoupçonnées, qui généreront leur propre potentiel de croissance. Cherchez un partenaire à la flexibilité éprouvée si vous voulez que vos objectifs futurs restent toujours à votre portée.

Extensibilité

Dans le monde de la musculation, le terme « extensibilité » désigne leur aptitude à s'étirer pour s'adapter à des mouvements et des charges variables. L'extensibilité a un rôle très similaire dans une solution CIAM.

Votre solution CIAM doit vous permettre d'ajouter facilement des personnalisations et des intégrations tierces à tout moment du flux d'identité : avant et après l'enregistrement d'utilisateur, après le changement de mot de passe, l'envoi de messages téléphoniques ou la création d'extensions personnalisées dans un environnement pro-code. Par exemple, vous pouvez configurer l'authentification multifacteur pour qu'elle se déclenche sur la page de connexion ou après, avec la réinitialisation du mot de passe, ou tout autre option, afin de personnaliser le niveau exact de friction requis pour assurer la sécurité des utilisateurs, tout en protégeant leur expérience d'utilisation de votre application.

L'extensibilité vous permet d'ajouter les capacités et les fonctionnalités personnalisées dont votre entreprise a besoin. S'il est certain qu'elle peut améliorer l'expérience utilisateur, elle accélère aussi la capture d'éclairages exploitables sur diverses organisations et fonctions internes.



Pour une entreprise, la réussite nécessite l'instrumentation et la contribution de plusieurs services, dont beaucoup ont des fonctions apparemment concurrentes:

- **Expérience numérique client:** Client 360°, expérience et personnalisation, outils analytiques et personnalisation Web, conversion des clients, support omnicanal
- **Systèmes clients, marketing et finance:** Applis marketing, CRM
- **Protection des données personnelles, conformité réglementaire, gouvernance** Protection des données personnelles et audits, conformité des informations personnelles identifiables (PII), réglementations de la protection des données personnelles, gestion des consentements
- **Sécurité/ protection:** Évaluation continue et adaptative des risques et de la confiance Protection DDoS, détection des fraudes, outils analytiques de la sécurité
- **Systèmes d'entreprise:** Intégration des données, MDM, veille économique

Heureusement, tous ces domaines sont alimentés et enrichis par votre solution CIAM. Par conséquent, vous pouvez utiliser la CIAM comme un outil pour créer un consensus : à condition de choisir un fournisseur d'identité capable de gérer vos besoins d'extensibilité les plus spécifiques.

> «Notre responsable clientèle m'a envoyé un message l'autre jour. Il me demandait : saviez-vous qu'Auth0 a une intégration Zendesk ?... il nous a suffit d'une réunion Zoom de 10 minutes pour la mettre en place.»
>
> — SHLOMI COHEN, ARCHITECTE SYSTÈME, KENSHOO

Une liste de contrôle de l'extensibilité

De nombreuses solutions CIAM se targuent d'être extensibles. Ce qui ne veut pas dire qu'elles ont réellement ce dont vous avez besoin pour votre situation spécifique. Voici une liste de contrôle rapide pour vous aider à reconnaître l'extensibilité dont vous avez besoin:

> «Les employés et les partenaires de T-Mobile utilisent tous les mêmes processus d'authentification Okta. Ce qui simplifie tout. Ils n'ont rien eu à apprendre ou à changer. En fait, ils ont eu moins à faire, une fois que nous avons mis la solution en place.»
>
> —WARREN MCNEEL,
> DIRECTEUR DE LA SÉCURITÉ DE L'ENTREPRISE, T-MOBILE

- **Mise en œuvre rapide de la fonctionnalité de base prête à l'emploi.** Mettez rapidement en place des applications pilotes et simples, avec un minimum d'installation/ configuration.
- **Options Low-code et No-code.** Déploiement en quelques clics, sans effort pour assurer la continuité et aucun temps d'arrêt pour les améliorations du produit.
- Options **conviviales pour développeurs** afin de coder efficacement des extensions (ex. Node.js). Permettre aux futurs développeurs de personnaliser leurs produits pour répondre à des utilisations imprévues.

- **Optimisation** pour équilibrer les priorités, notamment la sécurité/l'expérience utilisateur et la conversion/protection des données personnelles. Personnalisations pour équilibrer (ou optimiser) chacune de ces quatre priorités professionnelles.
- **Ouvert** aux fournisseurs d'écosystèmes tiers, aux communautés et aux sources de données/systèmes externes. Aucune plateforme unique ne peut répondre à toutes les utilisations. Optez donc pour un fournisseur qui offre plusieurs points d'intégration et d'extension pour les partenaires.
- Une échelle **globale** pour toutes les extensions, avec notamment les options de résidence des données, les lieux d'exécution et le choix du fournisseur cloud préféré. Par définition, les applications doivent être globalement disponibles, y compris les performances d'exécution des extensions. Cependant, les plateformes CIAM doivent aussi permettre de conserver les données au repos, afin de respecter les réglementations spécifiques sur la protection des données personnelles.

Sécurité

Traditionnellement, on pense que vous devez toujours choisir entre sécurité et commodité pour concevoir vos interactions clients et définir le niveau des efforts requis pour les protéger, ainsi que leurs données. Traditionnellement donc, on considère que la friction augmente avec la sécurité. Avec les scénarios modernes d'authentification multifactorielle (AMF), d'authentification multifacteur adaptative ou d'authentification continue, vous pouvez toujours modérer le risque sans donner envie à vos clients d'aller cliquer ailleurs.

Une position de sécurité forte renforce la confiance des clients

Votre gestion de la sécurité peut avoir un impact important sur vos résultats. Une étude réalisée en 2021 par **IBM-Poneman** indique que les coûts des violations de données avaient augmenté en moyenne de 4,24 millions USD par incident au plan global, avec une moyenne de 9,05 millions aux États-Unis. Ces coûts des violations de données incluent les amendes réelles et le préjudice réputationnel, qui peut motiver les clients à choisir des marques concurrentes.

De nombreuses entreprises pensent, à tort, que la sécurité des solutions CIAM ne concerne que la détection des fraudes. C'est-à-dire la seule garantie que les bonnes personnes ont accès aux bonnes données au bon moment. Ils sont enfermés dans un cadre de sécurité où les interactions avec les clients sont perçues comme un potentiel de pertes.

> «Grâce à Auth0, nous avons pu garantir la protection des données personnelles et la sécurité de partenaires de santé, couvrant plus de 10 millions de membres. Maintenant, les employés de nos partenaires utilisent leurs informations d'identification professionnelles pour se connecter aussi à Headspace.»
>
> — GEORGE TORRES, DIRECTEUR DE L'INGÉNIERIE, HEADSPACE

La gestion des données décentralisées est l'une des principales difficultés rencontrées dans le domaine de la CIAM. Pour la simple raison qu'il est très difficile de sécuriser ce que l'on ne connaît pas. Il est encore plus difficile d'appliquer les réglementations sur la protection des données personnelles lorsqu'elles vous imposent de fournir des informations personnelles à la demande du client.

Une forte posture de sécurité CIAM assure non seulement une vision centralisée du client, mais aussi une plus grande facilité de conformité aux exigences de la protection des données personnelles au niveau global. L'équilibre entre la sécurité et la commodité n'est plus une question de friction ou d'absence de friction, mais plutôt d'éléments générateurs de la confiance client à différentes étapes de son parcours.

Utiliser votre parcours client pour réduire les risques

Vos clients ont parfaitement conscience qu'ils vous confient des données de valeur. Le nombre croissant de réglementations sur la protection des données personnelles prouve aussi qu'ils connaissent les risques et leurs

conséquences. Des cyberattaques défilent presque quotidiennement dans leur fil d'actualité, souvent liées à des marques autrefois fiables. Mais le simple fait de devoir se souvenir de quelques **70 à 80 mots de passe** entraîne leur réutilisation systématique et une impatience croissante face à des processus d'enregistrement de plus en plus chronophages.

Les attaquants comptent sur le fait que les gens sont submergés par le volume et qu'ils réutilisent leurs mots de passe. C'est ainsi que votre site de commerce en ligne peut subir des attaques par bourrage d'identifiants de grande ampleur. Ces problèmes peuvent s'avérer coûteux, non seulement par les violations potentielles, les amendes et l'impact sur la réputation, mais aussi en raison de l'augmentation du coût de vos services.

Nous constatons que l'AMF transparente et à faible friction peut non seulement éviter les violations potentielles, mais peut aussi avoir un effet rassurant, lorsqu'elle intervient à la bonne étape du parcours du client. Elle peut être perçue comme exprimant votre volonté de protéger en continu les informations personnelles de vos clients et que vous êtes prêt à prendre les mesures nécessaires pour les protéger. De même, le positionnement judicieux d'un CAPTCHA, ce défi illustré qui permet de déterminer si un robot ou un humain tente d'accéder à un compte, peut également être considéré comme une protection positive.

> «Non seulement nous sommes confrontés à des cybercriminels bien plus déterminés, mais aussi à une gamme de technologies très étendue. En éliminant les anciennes solutions et en centralisant les services, nous généralisons les contrôles communs et nous pouvons gérer l'État comme une opération de cybersécurité d'entreprise.»
>
> —ADAM FORD, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, ÉTAT DE L'ILLINOIS

Votre solution CIAM doit améliorer votre posture de sécurité

Lorsque tout est en place, votre solution CIAM devrait améliorer votre posture de sécurité parce qu'elle est basée sur des normes ouvertes. Vos ingénieurs en sécurité (si vous en avez) peuvent alors voir et suivre clairement comment les données circulent dans votre système. Ce qui n'est pas le cas dans les solutions où les données passent par la boîte noire du code propriétaire.

Diverses réglementations relatives à la protection des données personnelles, telles que RGPD, CCPA, LGPD et APPI, exigent que vous compreniez comment vos fournisseurs tiers utilisent ou traitent les flux de données dans votre système. Avec les normes ouvertes, vous pouvez plus facilement comprendre ce que vous devez faire pour assurer votre conformité.

En outre, votre solution CIAM doit offrir des certifications essentielles telles que PCI, ISO20071, SOC 2 Type 2, HIPAA (pour les États-Unis) et Gold CSA Star. Elles confirment que vos contrôles de sécurité périodiques sont assurés par un fournisseur indépendant, au lieu de revendiquer la solidité de votre posture de sécurité.

Renforcer la protection et la satisfaction du client

La centralisation de l'identité assure votre protection chaque fois qu'un client se connecte à une application. Elle vous permet également de créer une expérience de marque unifiée (et mieux sécurisée). Vous aurez résolu le défi de la CIAM avec efficacité sans obliger vos développeurs à travailler sans cesse sur des implémentations de sécurité fastidieuses. Vous pourrez l'appliquer à plusieurs produits, avec une mise en œuvre finale n'exigeant que quelques minutes, rarement quelques jours, au lieu de plusieurs mois, voire plus.

Éclairages exploitables sur les clients

Des expériences personnalisées, plus agréables, peuvent faire la différence entre garder un client ou le perdre parce qu'il a trouvé ailleurs une interface plus rapide.

Supposons que dans votre café, un client consomme régulièrement du café et qu'il vous achète aussi des grains en ligne, depuis longtemps inscrit à votre programme de carte de fidélité. Mais comme votre système n'a pas l'avantage d'être interconnecté par une solution CIAM efficace, vous ne pouvez pas savoir que « otterdog459 » dans votre programme de fidélité est aussi « dolphinswimmer » lorsqu'il fait ses achats en ligne ! Ou que ce client a deux autres noms d'utilisateur/mots de passe dans la chaîne de cafés que vous êtes sur le point d'acheter, parce qu'il a oublié son mot de passe.

Comme sa réinitialisation a échoué, il en a créé un autre, après avoir perdu dix minutes à essayer de joindre le service d'assistance.

Vous ne pouvez pas non plus savoir que votre otterdog459/dolphinswimmer a accumulé une tonne de points de fidélité… et que votre fusion lui fait craindre que ces points s'évaporent, ou que ce qui valait six macchiatos au caramel se réduise à quatre tasses de café.

Sans une source unique de vérité, de faits confirmés, vous aurez de plus en plus de difficulté à comprendre vos clients. Ce niveau d'incertitude croissant peut les pousser vers un concurrent, plus pratique et plus convivial.

A Dignity Health a constaté que 86 % de ses hôpitaux ont amélioré la communication entre médecins et patients grâce aux portails de patients pilotés par Okta.

Pourquoi l'identité est la source unique et naturelle de vérité

Dans certains secteurs d'activité, comme la banque, avoir la certitude d'être en relation avec la bonne personne est une exigence fondamentale. Quels que soient vos besoins, plus vous avez accès à des données exploitables, meilleure sera la connaissance de vos clients, et plus vous serez capable de créer des expériences motivant leur fidélité.

«Exploitables» étant le mot clé de cette équation ! Vous avez peut-être accumulé un volume important de données sur vos clients, mais la création d'une visibilité à 360 degrés pose certains défis. Des données sont bloquées dans un CRM qui attend encore une mise à jour. D'autres ont été capturées par une appli écrite par un programmeur indépendant qui n'a ajouté aucun commentaire à son code.

Imaginons un instant que vous dirigez une compagnie d'assurances avec des filiales spécialisées dans l'assurance vie et la protection des biens. Vos données démographiques de base vous permettent de tirer un certain nombre de conclusions. Mais si vous saviez sur quels éléments vos clients cliquent avant de s'enregistrer, cela pourrait transformer votre offre de produits dès maintenant et dans cinq ans. Malheureusement, les données de vos marques d'assurance-vie et de protection des biens sont cloisonnées. Chaque marque ayant ses propres flux de connexion et d'inscription, elles ne génèrent que des quantités de données isolées.

Si les consommateurs ont migrés sur des plateformes en ligne pendant la pandémie, ils ont aussi changé de motivations, comme l'indique le récent rapport d'**Accenture** d'une enquête couvrant 25 000 consommateurs dans 22 pays. 50 % des personnes interrogées ont déclaré que la pandémie les avait amenées à repenser leurs valeurs. Sur ces 50 %, 72 % attendent de leurs fournisseurs qu'ils « comprennent et suivent l'évolution de leurs

besoins et objectifs en période de crise ». Nous avons ici une indication claire de la nécessité incontournable de comprendre les clients au fil du temps pour suivre et répondre à leurs attentes, au fil de leurs évolutions.

Si vous investissez des efforts considérables pour unifier vos données sans améliorer le flux d'inscription, vos données resteront toujours obsolètes. Chaque fois qu'un client clique, il ne fait en réalité qu'augmenter la quantité de données cloisonnées.

Augmenter les conversions en réduisant les frictions

Il est indispensable de comprendre l'activité de vos utilisateurs, et de ceux qui reviennent, pour identifier les modèles d'opportunité qui ont un impact spécifique sur vos taux de conversion et de rétention. Ces opportunités sont souvent révélées par la réduction des frictions.

Malgré la migration massive en faveur du commerce en ligne, la conversion continue de poser des défis. Début 2022, le **taux de conversion moyen des** plateformes de vente en ligne était de 1,53 %, soit une baisse de 0,32 % par rapport à l'année précédente. De nos jours, les clients n'ont pas la patience de remplir des formulaires d'enregistrement frustrants. Ce qui ne veut pas dire que cette impatience n'a pas pour vous certains avantages.

Pour réduire les frictions et leur impatience, vous pouvez leur permettre d'utiliser des connexions par réseau social, avec leurs identifiants de leurs applis préférées, comme Facebook ou Google.

L'entreprise de cybersécurité Snyk a estimé qu'avec l'authentification unique (SSO) d'entreprise et les connexions par réseau social, le taux de conversion des utilisateurs nouvellement inscrits pourraient atteindre 100 %.

Vos données, votre approche

Les solutions CIAM sont souvent confrontées au problème d'être conçues pour un groupe spécifique d'utilisateurs. Par exemple, les données les mieux adaptées aux besoins de vos équipes de marketing et de finance ne sont pas forcément les mêmes que celles dont votre équipe de sécurité a besoin pour assurer la sécurité de vos clients. Vos équipes

responsables de la protection des données personnelles et de la conformité ont besoin d'éclairages exploitables spécifiques. Alors que les priorités de votre équipe chargée de l'expérience numérique sont largement différentes.

Vous ne trouverez aucune solution CIAM conçue pour couvrir tous ces besoins. Il peut donc sembler judicieux de faire des compromis. Cependant, comme vous ne pouvez pas prévoir les données dont vos équipes auront besoin l'année prochaine, ou dans cinq ans, vous risquez de fermer la porte à des futures opportunités.

Vous avez donc besoin d'une solution CIAM extensible, intégrant un solide écosystème d'intégrations. Elle vous permettra d'exploiter vos informations selon l'approche que vous aurez définie, sans dépendre d'un seul fournisseur. Vous ne voulez évidemment pas découvrir après deux ans d'activité que vous avez dépassé les capacités de votre système et que vous ne pouvez pas aisément transférer vos précieuses données chez un autre fournisseur.

En finalité : Quelle que soit la façon dont vous souhaitez exploiter vos données clients, et pour réellement comprendre votre entonnoir, vous devez avoir accès à toute la richesse des informations injectées dans vos outils analytiques.

Coûts opérationnels

Traditionnellement, on pense que vous devez toujours choisir entre sécurité et commodité pour concevoir vos interactions clients et définir le niveau des efforts requis pour les protéger, ainsi que leurs données. Traditionnellement donc, on considère que la friction augmente avec la sécurité. Avec les scénarios modernes d'authentification multifactorielle (AMF), d'authentification multifacteur adaptative ou d'authentification continue, vous pouvez toujours modérer le risque sans donner envie à vos clients d'aller cliquer ailleurs.

Une position de sécurité forte renforce la confiance des clients

Toute interruption de l'activité pour assurer la maintenance de votre système d'identité peut provoquer des frictions qui pousseront vos clients vers des concurrents offrant un niveau de friction comparativement réduit. Mais aucun système de gestion de l'identité ne peut jamais être installé une fois pour toutes. Il doit forcément évoluer avec vos activités.

> «Je crois qu'on sous-estime trop souvent les exigences inhérentes à la gestion d'identité et de certaines de ses composantes intégrées dans la plateforme.»
>
> — JOHN MCKIM, VP DE LA TECHNOLOGIE DES PRODUITS, A CLOUD GURU

Protection contre les attaques

En tant qu'entreprise au service du consommateur, vous êtes une cible privilégiée pour les attaquants qui savent que vous protégez des éléments d'identité essentiels : noms, adresses et courriels, mais aussi informations de paiement.

Même si vous ne capturez que peu d'informations, les attaquants vous cibleront car les gens réutilisent leurs mots de passe. Une enquête de **Google-Harris** a constaté que 66 % des gens réutilisent des mots de passe pour accéder à plusieurs comptes. Dans une récente enquête de **LastPass**, 91 % des personnes interrogées ont déclaré qu'elles ont compris le risque, mais préfèrent réutiliser quand même les informations d'identification. Les attaquants le savent, et ils ont le temps et la puissance de calcul nécessaires pour exploiter ces données.

La fréquence des violations de données augmente constamment dans toutes les régions du monde. **Tenable**, une entreprise spécialiste de la cyber-exposition, a signalé la divulgation illégale de 40 milliards de dossiers en 2021, soit une augmentation de près de 78 % par rapport à l'année précédente.

Par conséquent, vous devez fournir régulièrement des mises à jour de sécurité des applications à vos clients afin de les protéger contre des attaques toujours plus nombreuses.

Les incontournables mises à jour

Outre les mises à jour destinées à protéger vos clients, les updates sont aussi indispensables pour offrir une nouvelle fonctionnalité ou ajouter des produits ou des modes de paiement supplémentaires. Si vous faites l'acquisition d'une marque (ou cinq), vous aurez besoin de les intégrer

d'une manière transparente et logique, et permettre à vos clients de faire facilement des découvertes sur mesure. Il peut aussi être nécessaire d'intégrer les fonctions apportées par de nouveaux partenaires. Vous pouvez aussi vous étendre dans une nouvelle région.

Chaque jour, la technologie évolue. Vous recevrez donc des mises à jour de tiers, qui peuvent ne pas convenir à votre calendrier d'exécution. Vous avez besoin d'une solution CIAM capable de suivre et d'intégrer les changements.

Limitation involontaire de votre stratégie commerciale

Votre équipe peut avoir développé une panoplie d'innovations fantastiques, susceptibles de générer une augmentation sans précédent des encaissements… mais si votre système CIAM a vieilli, fleuron dépassé de la génération précédente, il est devenu un obstacle au lieu d'être un moteur. Alors si vous devez dire à votre équipe que ses innovations devront attendre, aussi prometteuses soient-elles, vous risquez de perdre du temps et des talents. Ce que vous apporte aujourd'hui une solution CIAM n'est pas nécessairement ce dont vous aurez besoin dans six mois, un an ou cinq ans. Vous avez besoin d'une CIAM capable de suivre votre évolution, de favoriser l'innovation et la croissance au lieu de les bloquer.

Les processus manuels peuvent être coûteux

Pour toutes les entreprises technologiques, la recherche et le recrutement des talents est un défi incessant. Une fois ces talents intégrés dans votre équipe, ils auront comme cœur de métier la réalisation de votre objectif principal, en repoussant les limites de l'innovation, pour offrir davantage à vos clients.

Demander à vos développeurs internes de délaisser leur cœur de métier pour mettre au point une énième mise à jour, ou actualiser la protection des données personnelles, peut s'avérer coûteux en termes de coûts opérationnels, sans parler des opportunités perdues.

En particulier, si vos développeurs doivent coder en dur les modifications, au lieu d'une personnalisation complémentaire, vous devrez vous préparer à supporter un investissement en temps considérable. Vos développeurs peuvent être extrêmement talentueux, mais sans pour autant avoir une expérience même minime des complexités de l'identité en ligne. Leur demander de se mettre à la hauteur, et de suivre l'évolution du secteur de l'identité serait une dépense inutile.

Grâce aux rapports simplifiés et l'automatisation des politiques Okta, un vaste référentiel de codes logiciels dans le cloud a pu réduire de 90 % ses coûts de conformité, par rapport à sa solution bricolée précédente.

Augmentation des coûts liés à l'expérience client

Lorsque le produit est centré sur le consommateur, l'augmentation des coûts est plus probable, puisque l'attente a un impact direct sur l'expérience du client, augmente la friction et peut générer des réinitialisations de mot de passe coûteuses.

Une statistique souvent citée veut que la réinitialisation des mots de passe coûte jusqu'à 70 dollars par appel. Ce chiffre peut être largement plus élevé, selon le secteur d'activité. Multiplié par des millions de clients, le total peut vite devenir désagréablement impressionnant.

Coûts de certification

Des certifications, telles que SOC 2, HIPAA et ISO 27001, nécessitent un investissement initial pour les obtenir, en plus des coûts annuels pour les conserver. Mais leur absence peut constituer un frein à la croissance, en particulier lorsque vous ciblez des entreprises. « La plupart des entreprises Fortune 500 ne signeront pas avec vous, si vous n'avez pas les certifications attendues », affirme Adam Nunn, directeur principal de la gouvernance, des risques et de la conformité pour Auth0. « Cela peut représenter des coûts annuels très variables, allant de 25 000 dollars à plusieurs millions, selon la taille de l'organisation. »

Un fournisseur CIAM fiable apporte ses propres certifications qui couvrent la solution que vous achetez. Cela inclut l'investissement annuel dans des auditeurs tiers, les salaires du personnel chargé de la conformité, les outils de conformité internes (à l'exclusion des outils d'ingénierie et/ou des outils déployés pour la sécurité) et l'amélioration continue des processus. Ce qui pour vous élimine à la fois les efforts de certification et les coûts pour les clients.

Planifier pour maintenant et pour cinq ans dès maintenant

En évaluant les six domaines abordés dans ce guide, vous et votre équipe d'achat pourrez faire un meilleur choix, mieux adapté à vos besoins. La recherche des différenciateurs suivants pourrait faire la distinction entre une solution CIAM qui devient un obstacle après six mois ou un an, et la solution qui vous aidera réellement à vous développer et à innover.

Assurez-vous que tout le monde est sur même longueur d'onde

Comme une solution CIAM se retrouve au centre de tant de fonctions essentielles, vous risquez de créer accidentellement une technologie qui peut manquer de capacité à offrir un jeu réellement collectif. Mieux vaut revoir la liste ci-dessous et examiner votre structure organisationnelle particulière de manière plus systématique.

Vous pourrez alors mieux identifier les personnes qui doivent faire partie de votre équipe de prise de décision (ou qui pourraient avoir été oubliées par inadvertance).

Pour que votre CIAM soit un succès, vous devrez négocier un accord entre les équipes en charge:

- Gestion des produits
- Sécurité
- Systèmes d'entreprise
- Outils analytiques des clients et expérience numérique

- Protection des données personnelles, conformité réglementaire, gouvernance
- Outils analytiques/systèmes marketing et finance
- Service informatique/opérations IT

Nous vous suggérons ci-dessous quelques questions pour votre équipe de décision:

- Si certains décideurs penchent encore pour un développement en interne, avez-vous prévu un budget pour les compétences, la maintenance et la complexité croissante?
- Avez-vous identifié les principales parties prenantes de chacun des domaines énumérés ci-dessus? Certains manquent-ils encore dans l'équipe décisionnelle?
- Quelle est votre trajectoire de croissance? Avec quelle rapidité avez-besoin d'évoluer et d'intégrer de nouveaux partenaires/produits pour préserver votre flexibilité et votre capacité d'innovation?
- Dans quelle mesure la solution que vous proposez peut équilibrer les besoins contradictoires de la sécurité et de la commodité? Qu'avez-vous mis en place pour la protection des données personnelles et des revenus ? L'identité est une exigence commune à toutes les fonctions.
- Est-ce que tous ont compris les compromis que vous faites pour votre situation unique?

Forger un accord

Différentes équipes ayant forcément des besoins différents, vous pourriez avoir besoin de définir des critères spécifiques pour les départager et parvenir à un accord complet. Ces quatre différenciateurs peuvent vous aider à identifier la solution la plus flexible pour répondre aux besoins de chacun.

- **Une offre indépendante et neutre qui vous apporte plus de choix et une meilleure intégration avec vos solutions existantes.** Même si la CIAM peut faire des choses merveilleuses, il n'est cependant pas nécessaire d'abandonner ce qui fonctionne déjà pour vous. Une solution CIAM robuste est capable d'intégrer des applications et des systèmes existants en exigeant moins d'efforts manuels. Grâce à ses normes ouvertes, cette même solution vous évitera de dépendre de certains fournisseurs. Et vous devriez pouvoir utiliser votre solution CIAM avec le soutien de votre fournisseur cloud préféré.

- **Une solution complète et personnalisable offrant des expériences dignes de confiance, cohérentes et transparentes.** Votre entreprise est unique et ses besoins sont complexes et spécifiques. Nous vous invitons à rechercher une solution capable de supporter concrètement la création des expériences que vos utilisateurs finaux attendent aujourd'hui. Cette solution devra évoluer facilement selon vos besoins, que l'utilisateur final soit un consommateur, un client, un partenaire, un médecin, un vendeur, un étudiant ou un électeur.

- **Votre solution CIAM doit être facile à mettre en place, à utiliser et à maintenir.** Attendez-vous à bénéficier d'un déploiement, d'une maintenance et d'une administration simplifiés. Grâce à la réduction des efforts et du temps que vos ingénieurs consacreront au déploiement, à la configuration et au fonctionnement continu de votre CIAM, ils seront d'autant plus disponibles pour se concentrer sur l'amélioration de votre produit principal.

- **Vous avez besoin (comme vos utilisateurs finaux) d'une solution CIAM qui mérite toute votre confiance.** Toute faiblesse en termes de sécurité, de conformité et de disponibilité représente un risque pour l'expérience que votre marque propose. Une solution CIAM qui offre une fiabilité prouvée et une protection efficace contre les menaces, qui vous permet de répondre aux attentes en matière de conformité et de protection des données personnelles, sera un outil stratégique pour établir et maintenir votre réputation de marque de confiance.

Souhaitez-vous en savoir plus?

Pour résumer, la CIAM combine trois fonctions : faciliter l'inscription des clients, vendre des produits ou favoriser des interactions et fidéliser vos clients.

Si vous souhaitez obtenir de l'aide pour savoir comment mettre en œuvre votre solution CIAM facilement, en toute sécurité et transparence, n'hésitez pas à contacter notre équipe.

Auth0 fournit une plateforme qui permet d'authentifier, d'autoriser et de sécuriser les accès aux applications, aux appareils et aux utilisateurs. Les équipes de sécurité et de développement s'appuient sur la simplicité, l'extensibilité et l'expertise d'Auth0 pour que les fonctions d'identité répondent aux besoins de tous. En protégeant plus de 4,5 milliards de transactions de connexion chaque mois, Auth0 sécurise les identités pour que les innovateurs soient libres de créer. Auth0 permet aux grandes entreprises de fournir des expériences numériques de confiance et de qualité supérieure à leurs clients du monde entier.

Pour plus d'informations, visitez notre site Web **https://auth0.com** ou suivez **@auth0** sur Twitter.