

Information

Ping
Identity.

Le guide d'achat sur l'identité des clients

Comment choisir une solution de gestion des identités et des accès des clients qui vous aide à atteindre vos principaux objectifs business



GUIDE D'ACHAT

Information

Female
Age 45

INTRODUCTION

Offrir des expériences digitales transparentes et sécurisées à vos clients est devenu indispensable pour votre entreprise. Le succès extraordinaire des sites de commerce comme Amazon et AliExpress est la preuve qu'en matière de shopping en ligne, ce que les clients désirent, c'est la simplicité et la praticité. Les événements comme la pandémie mondiale de la COVID-19 accélèrent la progression de cette tendance et renforcent l'idée que l'expérience numérique des clients constitue le champ de bataille sur lequel vous allez gagner ou perdre des parts de marché.

Alors que de plus en plus de clients franchissent le seuil numérique de votre enseigne, la capacité à fournir une visite homogène et agréable à vos utilisateurs devient une nécessité qui peut faire la différence dans la réalisation de vos objectifs et afin de rester compétitif. Entre la création de compte, la connexion, le service clients et la gestion des préférences, vos clients souhaitent simplement pouvoir visiter votre site sans anicroche et en toute sécurité. Si ce n'est pas le cas, ils n'hésiteront pas à aller voir ailleurs.

« Augmenter l'attractivité d'une marque peut se faire en entretenant une communauté (par exemple, ASOS Marketplace), en mettant en place des programmes de fidélité et en proposant des **expériences mobile et bureau homogènes** »

Présentation du marché numérique, commerce électronique international, Statista

Votre manière de concevoir, gérer et déployer l'identité de vos clients peut faire de leur visite un échec total ou une franche réussite. Le CIAM (gestion de l'identité et des accès pour les clients) vous permet d'homogénéiser le parcours de vos clients, ce qui est fondamental si l'un des objectifs stratégiques de votre organisation est de parvenir à une croissance continue en termes d'acquisition et de fidélisation des clients ainsi que de revenus.

Ce guide d'achat vous aidera à préciser vos besoins en CIAM par rapport à vos priorités commerciales afin de déterminer au mieux quelles solutions vous conviendront. Continuez votre lecture pour comprendre en profondeur le principe d'identité client et le rôle que le CIAM joue dans l'amélioration de la sécurité, de la confidentialité et du ressenti des clients.

« En 2022, le CIAM sera un **élément capital** d'une stratégie compétitive d'expérience utilisateur pour 85 % des organisations, comparé à 40 % aujourd'hui. »

« Aperçu de la technologie en gestion de l'identité et accès pour les clients », Gartner, mai 2020

POURQUOI VOUS AVEZ BESOIN D'UNE GESTION D'IDENTITÉ DES CLIENTS

L'identité client peut vous aider à garantir que chaque étape du parcours de vos clients sera fluide et sécurisée mais aussi à leur fournir l'expérience client à laquelle ils aspirent. Rien que cela en fait une obligation pour les entreprises qui souhaitent rester compétitives et accorder la priorité au client.

Mais si la gestion de l'identité client peut potentiellement améliorer fortement les visites de vos clients (et les profits de votre organisation), le diable se cache dans les détails. Sans stratégie bien réfléchie, les initiatives liées à l'identité peuvent engendrer des gênes superflues. Si vos clients trouvent les processus d'inscription, d'authentification et de gestion des préférences lourds, votre transformation pourrait ne pas produire les résultats escomptés. Et vos clients pourraient aller voir ailleurs.

Avant de commencer votre périple dans le domaine du CIAM, il vous faut établir les desiderata de vos clients. C'est en comprenant leurs besoins que vous pourrez manier le pouvoir de l'identité client à bon escient et à votre avantage. Si cette compréhension peut sembler difficile à acquérir, elle se résume en vérité en deux points :

Satisfaire vos clients

- Sachez reconnaître vos clients sur les différents canaux. N'attendez pas d'eux qu'ils modifient leur compte ou leurs paramètres plus d'une fois.
- Rendez les processus d'inscription et de connexion aussi rapides et fluides que possible. Ne compliquez pas les choses plus que nécessaire.

Protéger et respecter vos clients

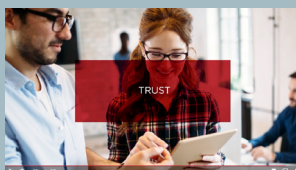
- Prenez votre rôle d'intendant au sérieux et protégez les données à caractère personnel de vos clients. Ne les exposez pas à des risques d'usurpation d'identité ou à des fuites.
- Soyez transparent avec vos clients et donnez-leur le contrôle sur leurs données à caractère personnel. Respectez leur droit à la vie privée.

Lorsqu'elle est appliquée correctement, la gestion de l'identité des clients facilite la satisfaction, la protection et le respect de vos clients. Et une fois que vous avez compris cela, vous avez posé les bases pour construire une expérience client (CX) exceptionnelle.

Ce n'est pas un secret : ce qui fera la différence avec vos concurrents, c'est la CX. Vous ne devriez pas non plus être surpris par le fait que vous pouvez planifier votre gestion de l'identité des clients directement d'après votre expérience client, dès l'inscription et à toutes les étapes de leur parcours.

Une gestion de l'identité client alliant souplesse et robustesse est indispensable pour que les visites de vos clients se déroulent de manière commode, homogène et sûre. Une fois cela atteint, vous pourrez survoler la concurrence et aider votre organisation à remplir ses objectifs critiques, parmi lesquels :

- Gagner plus de clients
- Fidéliser les clients existants
- Augmenter le chiffre d'affaires
- Accroître la fidélité des clients
- Gagner la confiance de vos clients



[Regardez la vidéo](#) pour découvrir comment rendre la visite de votre site agréable grâce à la gestion d'identité client.

COMMENT BIEN SE LANCER DANS LE CIAM

Choisir la solution de gestion d'identité des clients adéquate passe par une bonne compréhension des objectifs les plus importants de votre organisation. Contrairement à l'IAM destiné aux employés, l'identité client a des implications sur les revenus, elle est donc directement liée à vos objectifs stratégiques généraux et à des indicateurs de performance clés comme :

- L'acquisition des clients
- La rétention des clients
- L'augmentation du chiffre d'affaires
- La fidélité des clients
- La confiance des clients

Une fois que votre société a déterminé les objectifs et indicateurs auxquels elle accorde le plus d'importance, vous pouvez choisir une solution qui soit capable de vous apporter ce que vous désirez.

Comme la figure 1 le montre, les capacités en CIAM ont une corrélation directe avec les différentes étapes du parcours d'un client. Par exemple, l'inscription, l'authentification, le self-service et l'assistance influent directement sur l'acquisition et la rétention des clients. Ainsi, si ce sont des indicateurs capitaux pour votre organisation, vous allez devoir prioriser ces capacités durant votre sélection d'une solution de gestion d'identité des clients. Suivant le même principe, afin de permettre un accroissement du chiffre d'affaires, vous devriez plutôt vous concentrer sur le self-service, la personnalisation et l'assistance.



Figure 1 : l'identité client influe sur toutes les phases du parcours de votre client et est directement liée aux principaux objectifs commerciaux de beaucoup d'organisations.



Pour en savoir plus sur la manière dont le CIAM soutient le parcours des clients, lisez le [guide complet des solutions IAM destinées au client](#).

CHOISIR VOTRE APPROCHE CONCERNANT LA GESTION DE L'IDENTITÉ DES CLIENTS

Pendant que vous commencez à déterminer ce que votre solution de CIAM doit comprendre, pensez à considérer l'étendue de vos besoins en gestion de l'identité des clients. En fonction de vos objectifs, de vos obligations et de votre maturité actuelle, vous allez devoir identifier si des améliorations petit à petit suffiront ou s'il serait plus intéressant de subir une transformation à grande échelle.

Des améliorations par étapes peuvent-elle suffire ?

Si votre organisation a besoin d'un succès immédiat pour commencer à améliorer immédiatement l'expérience de ses clients, ou pour corriger un endroit particulièrement inadapté de son parcours utilisateur, une approche par étapes pourrait être suffisante. En se limitant à l'amélioration d'une seule chose à la fois, vous y arriverez plus rapidement. Vous pourrez concentrer vos efforts sur un seul endroit et apprendre sur le tas.

Par exemple, comme sur la figure 2, vous pourriez estimer que la personnalisation est la première chose à modifier pour améliorer votre chiffre d'affaires. Dans ce cas, il vous faudrait travailler à créer un profil de client unifié, afin que l'expérience soit la plus homogène possible quel que soit le canal emprunté.

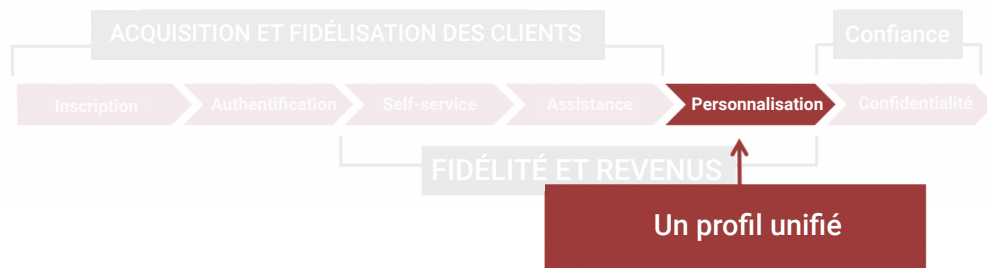


Figure 2 : Une approche par étapes du CIAM implique la mise en place d'un seul produit ou capacité pour répondre rapidement à un besoin opérationnel.

Si opter pour une approche par étapes peut payer assez vite, elle peut aussi vous ralentir par la suite. En limitant votre capacité à vous rendre compte de l'impact véritable de la gestion d'identité client sur vos revenus, l'acquisition, la rétention et la fidélisation des clients, vous favorisez des gains à court terme aux dépens d'une influence sur le long terme.

Choisir une solution simple comporte aussi des risques. Vous pourriez vous retrouver avec des systèmes disparates que vous ne pourrez pas intégrer plus tard, quand vous en aurez inévitablement besoin. Si vous voulez la garantie de rencontrer un succès continu via une approche par étapes, assurez-vous que les capacités de votre prestataire couvrent davantage que vos besoins immédiats. Il vous faudra un partenaire avec une approche holistique et une large gamme de fonctionnalités pour être sûr que vos profits immédiats ne soient pas contrecarrés par de futurs défis.

Ou une transformation à grande échelle produirait-elle de meilleurs résultats ?

Si vous n'avez pas besoin d'obtenir des résultats rapides, une transformation à grande échelle sera peut-être plus indiquée. Cela reste une approche focalisée, mais au lieu de tout concentrer sur un point en particulier, vous vous attaquerez d'abord à une étape du parcours utilisateur.

Les transformations à grande échelle entraînent en général la mise en place d'une solution intégrale de CIAM qui combine toutes les fonctionnalités CIAM nécessaires à l'amélioration d'une étape particulière du parcours utilisateur. Le parcours utilisateur est habituellement composé de trois étapes. Selon quelle étape s'accordera le mieux à vos priorités, vos initiatives CIAM se résumeront ainsi :

Acquisition et rétention

Pour gagner et conserver plus de clients, concentrez-vous sur des choses comme l'inscription facile, le Single Sign-on (SSO, ou méthode de connexion unique), les fonctionnalités de type self-service et l'assistance (figure 3).

Fidélité et revenus

Afin d'encourager la croissance du chiffre d'affaires et la fidélisation des clients, mettez l'accent sur des options d'assistance et de self-service intuitives, ainsi que sur la personnalisation des expériences multicanal pour que les clients continuent d'interagir avec votre marque.

Confiance

Pour gagner la confiance de vos clients, donnez-leur la maîtrise totale sur leurs données, tout en les protégeant (ainsi que votre marque) contre des menaces de type fuite de données, usurpation d'identité et fraude à la consommation.

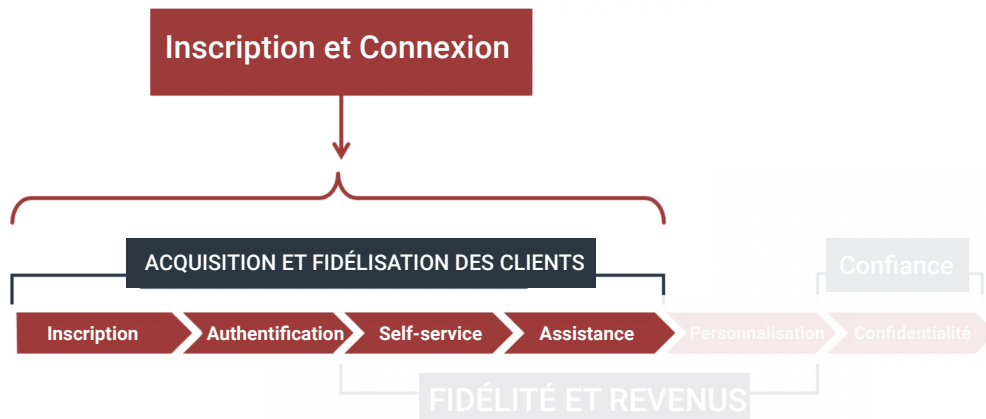


Figure 3 : Pour gagner et conserver plus de clients, concentrez-vous sur l'amélioration de vos processus d'inscription et de connexion.

En choisissant cette approche, vous restez orienté vers un objectif clair, mais à un niveau supérieur, qui vous laissera faire des améliorations plus conséquentes et ayant un impact commercial tangible. C'est pour cela que nombre de sociétés trouvent que cette approche convient davantage à leurs objectifs. Avec la bonne solution CIAM, vous pourriez même vous rendre compte des bénéfices d'une transformation à grande échelle plus vite que vous ne l'imaginez.

« Nous ne croyons pas qu'une solution à utilisation unique convienne à l'identité et la gestion des accès. La **flexibilité de la plateforme CIAM** de Ping permet aux clients d'avoir un profil sécurisé et unifié ainsi qu'un ensemble d'identifiants pour accéder à tous leurs services ».

Stephanie Kesler, spécialiste technologie / architecte d'entreprise, [GCI](#)



ÉTABLIR VOS CRITÈRES D'ÉVALUATION

Après que vous avez clarifié vos objectifs commerciaux et emporté l'adhésion pour aller de l'avant, vous devez identifier les fournisseurs à examiner. Lorsque vous évaluez un fournisseur, prenez les éléments suivants en considération :

- Depuis combien de temps ce fournisseur travaille-t-il dans ce secteur ?
- Ce fournisseur est-il un leader du secteur ?
- Ce fournisseur a-t-il fait preuve d'expertise sous la forme d'exemples de réussite des clients et de témoignages ?
- Ce fournisseur est-il impliqué dans la recherche et le développement continus pour améliorer les produits et satisfaire l'évolution des exigences du secteur et des clients ?
- Ce fournisseur propose-t-il une formation solide, une assistance et une communauté d'utilisateurs active ?

Il vous faudra aussi évidemment évaluer la capacité de chaque prestataire à remplir vos objectifs et exigences spécifiques. Dans ce but, nous vous avons fourni un résumé des capacités CIAM, ainsi que des explications justifiant l'importance de chacune d'elles.

Les critères sont présentés de manière à maintenir l'alignement entre initiatives commerciales classiques et capacités de gestion d'identité client. Si vous établissez vos critères de sélection à l'aide de cet axe, vous pourrez privilégier les capacités qui auront le plus grand impact sur les objectifs particuliers à votre organisation.

Acquisition et rétention



Ces critères concernent l'évaluation de la capacité d'un fournisseur à faciliter la vie de vos clients pour effectuer des actions comme s'inscrire, réinitialiser le mot de passe et résoudre les problèmes rencontrés.

CRITÈRE D'ÉVALUATION	POURQUOI C'EST IMPORTANT
Le fournisseur propose-t-il un SSO (Single Sign-on, ou méthode de connexion unique) fédéré ?	Vos clients s'attendent à avoir accès à toutes vos applications sans être obligés de se souvenir d'un ensemble d'identifiants différent pour chacune d'elles. Répondez à leurs attentes en leur fournissant un moyen de connexion pratique et constant grâce au SSO fédéré.
Le fournisseur propose-t-il une authentification sociale ?	Facilitez l'inscription et l'authentification de vos clients en leur donnant la possibilité d'employer les identifiants qu'ils utilisent sur leurs réseaux sociaux (comme Facebook ou Google).
Le fournisseur propose-t-il la possibilité de récupérer des comptes et une politique de mots de passe commode ?	La plupart des clients finiront par oublier leur mot de passe à un moment. Mettez en place un système simple et sûr de récupération de compte en appliquant les pratiques exemplaires en la matière ainsi que des politiques de mots de passe centralisés.
Le fournisseur prend-il en charge plusieurs formes d'authentification multifacteur (MFA) ?	Afin que la sécurité de tous les acteurs soit assurée, il est nécessaire que vos clients disposent d'options pratiques pour utiliser le MFA. Les prestataires doivent prendre en charge des méthodes telles que l'utilisation de mots de passe à usage unique délivrés par e-mail ou SMS, de certificats logiciels, de clés FIDO, etc.
Le fournisseur prend-il en charge la norme FIDO ?	Le FIDO permet aux clients d'utiliser des paires d'identifiants stockées sur un appareil considéré comme de confiance. C'est une pratique sûre et commode qui se répand de plus en plus, et qui pourrait à terme remplacer les mots de passe.
Le fournisseur intègre-t-il le MFA à votre propre appli mobile ?	Augmentez le niveau de sécurité pour vos clients en transformant votre appli mobile en un second facteur d'authentification, à l'aide de notifications push. Elles offrent plus de sécurité et de commodité que beaucoup d'autres formes de MFA.
Le fournisseur prend-il en charge l'authentification sans mot de passe ?	L'authentification sans mot de passe est en plein essor et pourrait bien devenir un incontournable pour certains cas d'utilisation. Demandez à votre prestataire s'il prend en charge l'authentification sans mot de passe pour que vous soyez paré à toute éventualité.
Le fournisseur autorise-t-il les politiques d'authentification reposant sur l'analyse des risques ?	Malgré tous vos efforts pour le rendre le moins gênant possible, le MFA restera toujours une friction pour l'utilisateur. Des politiques intelligentes qui ajustent à la hausse ou à la baisse la demande de MFA en fonction du risque permet de n'introduire cette friction que lorsque la requête l'oblige.
Le fournisseur propose-t-il des API qui confient aux équipes d'UX le contrôle intégral sur les expériences d'authentification et d'inscription ?	Représenter la marque de manière homogène, c'est un élément capital qui contribue à rendre exceptionnelle l'expérience du client, et quelque chose qui a demandé à votre société beaucoup de travail. Vérifiez que votre fournisseur permette à vos équipes UX de conserver la main sur l'inscription et l'authentification dans le but d'assurer une représentation homogène de votre marque.

Fidélité et revenus



Ces critères concernent l'évaluation de la capacité d'un fournisseur à faciliter la vie de vos clients pour effectuer des actions comme s'inscrire, réinitialiser le mot de passe et résoudre les problèmes rencontrés.

CRITÈRE D'ÉVALUATION	POURQUOI C'EST IMPORTANT
Le fournisseur propose-t-il des fonctionnalités de gestion des préférences ?	Permettre à vos clients de définir explicitement leurs préférences est une nécessité. Quand elles sont stockées dans un profil client unifié, l'expérience que vous fournissez sera à la fois constante et personnalisée sur tous les canaux.
Le répertoire du fournisseur peut-il stocker des données non structurées ?	Les données que vous allez collecter sur vos clients peuvent être diverses et inclure des données non structurées comme des empreintes digitales de navigateur. Les applications doivent être capables de stocker des ensembles de données complexes et des blobs JSON.
Le fournisseur permet-il d'ajouter des attributs personnalisés aux applis facilement ?	Vous devez pouvoir ajouter simplement des attributs personnalisés à vos applis, sans avoir besoin de recourir à des migrations schématiques risquées qui affecteraient potentiellement d'autres applications.
Le fournisseur propose-t-il de la synchronisation de données bidirectionnelle en temps réel ?	La synchronisation de données bidirectionnelle en temps réel vous autorise à rassembler des silos d'identité disparates dans le but de créer un profil unifié. Elle réduit aussi les risques et évite les interruptions de service.
Les applis ont-elles accès au profil du client via des API REST ?	Les protocoles historiques, comme le LDAP, sont nécessaires pour communiquer avec les répertoires existants et créer un profil unifié, mais les applis modernes préfèrent passer par des API pour accéder aux données des clients. Un profil unifié doit pouvoir proposer ces API.
Le fournisseur intègre-t-il le MFA à votre propre appli mobile ?	Augmentez le niveau de sécurité pour vos clients en transformant votre appli mobile en un second facteur d'authentification, à l'aide de notifications push. Elles offrent plus de sécurité et de commodité que beaucoup d'autres formes de MFA.
Le fournisseur sait-il gérer une échelle et une performance extrêmes et justifier son expérience en la matière ?	Si votre profil unifié n'est pas évolutif, il sera susceptible de ne plus fonctionner, empêchant ainsi vos clients de se connecter ou d'accéder à leurs données. Les prestataires doivent être capables de prendre en charge le stockage de millions d'identités et de milliards d'attributs, même dans des scénarios de fréquentation maximale impliquant des centaines de milliers d'utilisateurs en même temps, pour répondre correctement à tous les cas d'utilisation. Ils doivent en outre fournir des témoignages de clients qui attestent que la disponibilité et la latence restent optimales lors des pics de fréquentation.

Confiance



Inscription

Authentification

Self-service

Assistance

Personnalisation

Confidentialité

CONFIANCE

Ces critères d'évaluation des fournisseurs se concentrent sur la façon dont ils peuvent protéger la vie privée de vos clients et garantir la sécurité à tous les niveaux, y compris en empêchant les fraudes, les usurpations d'identité et les fuites de données.

CRITÈRE D'ÉVALUATION	POURQUOI C'EST IMPORTANT
Le fournisseur propose-t-il le contrôle de l'accès aux applications et aux API ?	Vous devez être capable de gérer le contrôle des accès à des URL et API spécifiques de manière centralisée. Les fournisseurs devraient pouvoir vous fournir des politiques de contrôle d'accès contextuel centralisées à cet effet.
Le fournisseur prend-il en charge une autorisation dynamique précise afin de respecter les réglementations relatives à la confidentialité ?	Les réglementations assurant le respect de la vie privée sont nombreuses et peuvent varier selon chaque organisation, secteur d'industrie, emplacement géographique, etc. Les solutions CIAM doivent comprendre des politiques de confidentialité à gestion centralisée dans le but de mettre en œuvre le consentement du client et de régir le partage de données, attribut par attribut, pour chaque appli.
Le fournisseur propose-t-il une vision approfondie du trafic des API pour détecter les menaces potentielles ?	Derrière chaque appli, il y a des API qui peuvent être exploitées et causer une faille de sécurité. Il vous faut une solution CIAM qui surveille l'intégralité du trafic API afin de repérer les comportements potentiellement malveillants et d'empêcher les attaques informatiques.
Le fournisseur peut-il stocker les données utilisateur dans plusieurs régions pour respecter les exigences en matière de souveraineté des données ?	De nombreuses régions géographiques disposent de règles qui imposent le lieu de stockage des données utilisateur. Puisque cela dépend du lieu de résidence de vos clients (et non de votre entreprise), un fournisseur identité capable de répondre aux contraintes de souveraineté des données est indispensable.
Le fournisseur peut-il récupérer et entreposer l'enregistrement du consentement des clients de manière à ce qu'il puisse être inspecté si besoin ?	Lorsque vous recueillez le consentement d'un client, vous devez le faire de manière à ce qu'un audit puisse être effectué. Votre prestataire doit pouvoir stocker l'heure de collecte des données, les preuves de cette collecte (comme une adresse IP) et d'autres renseignements nécessaires en cas d'audits privés.
Le fournisseur peut-il faire respecter le consentement des clients ?	De nombreux fournisseurs se contentent de réfléchir à leur manière de recueillir le consentement. Cela les amène malheureusement à laisser diverses équipes d'application écrire un code qui garantit la bonne mise en œuvre du consentement. Si votre organisation est de grande ampleur ou en pleine croissance, vous allez vouloir être capable de faire respecter le consentement de manière centralisée.
Le fournisseur sait-il gérer une échelle et une performance extrêmes et justifier son expérience en la matière ?	Si votre profil unifié n'est pas évolutif, il sera susceptible de ne plus fonctionner, empêchant ainsi vos clients de se connecter ou d'accéder à leurs données. Les prestataires doivent être capables de prendre en charge le stockage de millions d'identités et de milliards d'attributs, même dans des scénarios de fréquentation maximale impliquant des centaines de milliers d'utilisateurs en même temps, pour répondre correctement à tous les cas d'utilisation. Ils doivent en outre fournir des témoignages de clients qui attestent que la disponibilité et la latence restent optimales lors des pics de fréquentation.

CRITÈRE D'ÉVALUATION	POURQUOI C'EST IMPORTANT
Le fournisseur chiffre-t-il les données à chaque stade et met-il en œuvre d'autres pratiques recommandées concernant la sécurité en couches de données ?	Afin de garantir à tout instant la protection des données de vos clients, elles doivent être chiffrées dans tous leurs états : au repos, en mémoire et en mouvement.
Comment le fournisseur vous protège-t-il de menaces internes ?	Les personnes malveillantes internes peuvent constituer une menace non négligeable, quelle que soit la taille et le type de votre organisation. Demandez à votre fournisseur quels garde-fous il met en place pour contrecarrer les attaques venant de l'intérieur, comme les alertes en cas d'activité admin suspecte, les fichiers-journaux scellés et les limites d'enregistrement admin.

Conditions fondamentales

En plus d'évaluer comment un fournisseur pourra vous aider à atteindre vos objectifs commerciaux, il vous faudra aussi vérifier qu'il propose un certain nombre de fonctionnalités indispensables. Voici quelques critères de base à considérer, peu importe vos ambitions.

CRITÈRE D'ÉVALUATION	POURQUOI C'EST IMPORTANT
Le fournisseur prend-il en charge les standards ouverts ?	Il est vital pour une plateforme moderne d'identité client de gérer les standards ouverts tels que SAML, SCIM, OAuth ou OpenID Connect afin que la solution soit polyvalente et extensible.
Le fournisseur sait-il se connecter à des applications personnalisées qui ne sont pas basées sur des standards ?	Si votre plateforme doit absolument être compatible avec les standards, ce n'est pas le cas d'un grand nombre d'applications côté client. Votre prestataire devrait être capable de se connecter à ces applications et de fournir un accès simple à n'importe quelle propriété numérique de votre portfolio.
Le fournisseur prend-il en charge une sécurité forte de bout en bout sur chaque couche ?	Pour garantir la sécurité des données sensibles, votre prestataire CIAM doit pouvoir proposer une sécurité renforcée lors de l'authentification, au niveau des couches application et API comme de celle des données.
Le fournisseur propose-t-il des pratiques recommandées, des modèles d'appli et des UI prêts à l'emploi ?	Parvenir à une expérience client sûre et homogène est incontournable. Votre fournisseur doit vous faciliter la tâche à ce sujet en mettant à votre disposition des outils et ressources qui vous permettront à coup sûr d'y arriver, comme de la documentation complète sur les API, des modèles d'appli et des kits d'intégration prêts à l'emploi pour que vous soyez opérationnel le plus vite possible.
Le fournisseur peut-il coexister avec vos systèmes préexistants, pour vous permettre d'effectuer une migration étape par étape vers une solution CIAM plus moderne ?	Dans le cas des grandes entreprises, il est en général impossible de tout remplacer d'un coup. Lorsque votre fournisseur est à même de permettre une migration par étapes, en coexistant avec le système déjà en place, vous réduisez fortement les risques, notamment celui de l'indisponibilité.

CRITÈRE D'ÉVALUATION	POURQUOI C'EST IMPORTANT
Le fournisseur propose-t-il plusieurs options de déploiement pour que vous puissiez installer la gestion d'identité à l'endroit où vous en avez besoin ?	Vous devez être libre de déployer une gestion d'identité client où vous voulez, si vous désirez répondre à vos propres besoins. Un prestataire doit pouvoir vous fournir plusieurs options de déploiement, y compris la simplicité d'une solution IdaaS mutualisée, la configurabilité d'une solution gérée « single-tenant » ou la personnalisation d'une solution locale.
Le fournisseur propose-t-il des options de déploiement IDaaS (Identity as a service) « single-tenant » et mutualisées ?	Nombre d'organisations privilégient les déploiements sur des clouds qui sont gérés à leur place par une autre entité. Si c'est votre cas, il vous faudra un fournisseur dont les possibilités de déploiement IdaaS correspondent à vos besoins (qu'elles soient single-tenant ou mutualisées), afin que vous gardiez le contrôle nécessaire sur votre environnement.
Le fournisseur a-t-il une longue liste d'intégrations prêtes à l'emploi ?	Beaucoup de fournisseurs considèrent l'archivage des mots de passe ou la « prise en charge du SAML » comme des intégrations ; enquêtez un peu plus pour vérifier que ses intégrations ont les reins assez solides pour vos environnements et vos cas d'utilisation.
Le fournisseur peut-il déployer sa solution dans des clouds privés ?	Certaines organisations souhaitent conserver un contrôle total sur leur solution de gestion d'identité, en la mettant en œuvre dans un environnement qu'elles maîtrisent intégralement (que ce soit sur un cloud privé ou dans leurs locaux). Si c'est votre cas, vérifiez bien que votre fournisseur puisse se plier à cette exigence.
Le fournisseur prend-il en charge la conteneurisation et l'orchestration pour DevOps ?	En ce qui concerne les déploiements sur cloud privé comme ceux sur site, la prise en charge de la conteneurisation avec Docker et de l'orchestration avec des outils comme Kubernetes est capitale pour assurer un déploiement et une mise à l'échelle efficaces de votre solution de gestion d'identité client.
Les modèles de déploiement du fournisseur peuvent-ils fonctionner ensemble ?	Dans certains cas, des entreprises auront besoin de déployer leur solution dans des environnements de plusieurs types. Parfois, elle voudront un IdaaS single-tenant ou mutualisé pour quelques applis alors que d'autres applis vitales seront dans un cloud privé ou un environnement local. Si vous avez ce type de besoins, assurez-vous que la solution d'identité de votre fournisseur reste unie durant les déploiements sur plusieurs environnements.

Évaluation des fournisseurs et des solutions

Après avoir déterminé vos critères d'évaluation, organisez-les de manière à faciliter la comparaison entre vos potentiels fournisseurs. L'utilisation d'un feuillet Excel ou d'un Google Sheet peut s'avérer judicieuse. Nous vous suggérons de commencer par créer une ligne pour chacun des critères d'évaluation. Ajoutez ensuite des colonnes pour chaque fournisseur à évaluer. Vous pouvez évaluer chaque fournisseur selon sa capacité à répondre à vos critères, via un système à points similaire à celui-ci :

- 0 = Ne répond pas à l'exigence
- 1 = Répond de manière limitée à l'exigence
- 2 = Répond partiellement à l'exigence
- 3 = Répond à l'exigence, voire la surpasse

Avec ce système, évaluez chaque fournisseur de 0 à 3 pour chacun de vos critères. Faites ensuite le total de points pour chaque fournisseur et constatez lequel est le meilleur.

CHOISIR LA SOLUTION DE GESTION D'IDENTITÉ CLIENT ADAPTÉE À VOS BESOINS

Le choix d'une solution d'identité client est une décision importante, et il n'existe pas de solution universelle en la matière. La première étape consiste à identifier les principaux objectifs de votre organisation et ses critères de réussite. Pesez le pour et le contre entre une approche par étapes et une transformation à grande échelle. Ensuite, vous pourrez mettre à profit la compréhension des fonctionnalités de gestion de l'identité des clients que vous venez d'obtenir grâce à ce guide pour bien privilégier une solution qui correspondra à votre situation particulière.

« Établir une fonction de gestion d'identité numérique a créé une base fondamentale grâce à laquelle nous pouvons proposer à nos clients une **expérience homogène**, quel que soit le canal qu'ils aient choisi. Ping a aidé BNZ à effectuer sa transition vers le monde du numérique en **donnant à nos clients le contrôle de leur identité** ».

Stephen Bowe, directeur des applications et du numérique, [Bank of New Zealand](#)

Si, comme beaucoup d'autres, vous avez pour tâche d'identifier les différentes solutions d'identité client, pensez à consulter des ressources analytiques objectives et impartiales, comme Magic Quadrant for Access Management (Gartner, 2020), pour découvrir les recommandations des experts du secteur.



Pour en apprendre davantage sur les fonctionnalités CIAM primordiales et sur ce que vaut Ping Identity, procurez-vous un exemplaire gratuit de [Magic Quadrant for Access Management \(Gartner, 2020\)](#).

À PROPOS DE PING IDENTITY : Ping Identity est un pionnier des solutions intelligentes de gestion des identités. Nous aidons les entreprises à mettre en place une sécurité des identités Zero Trust et des expériences utilisateur plus personnalisées et plus fluides. La plate-forme Ping Intelligent Identity™ fournit aux clients, employés, partenaires et, de plus en plus, aux objets connectés, un accès aux API et aux applications cloud, mobiles, SaaS et sur site, tout en gérant les données d'identité et de profil à l'échelle de l'entreprise. Plus de la moitié des entreprises du classement Fortune 100 fait confiance à notre expertise en matière d'identités, à notre position de leader sur les standards ouverts, et à notre partenariat avec des sociétés comme Microsoft et Amazon. Nous proposons des options flexibles permettant d'étendre les environnements hybrides et d'accélérer les projets de transformation digitale des entreprises grâce à des fonctions d'authentification multifacteur, de gestion des accès, de sécurisation intelligente des API, de répertoire et de gouvernance des données. Rendez-vous sur www.pingidentity.com.