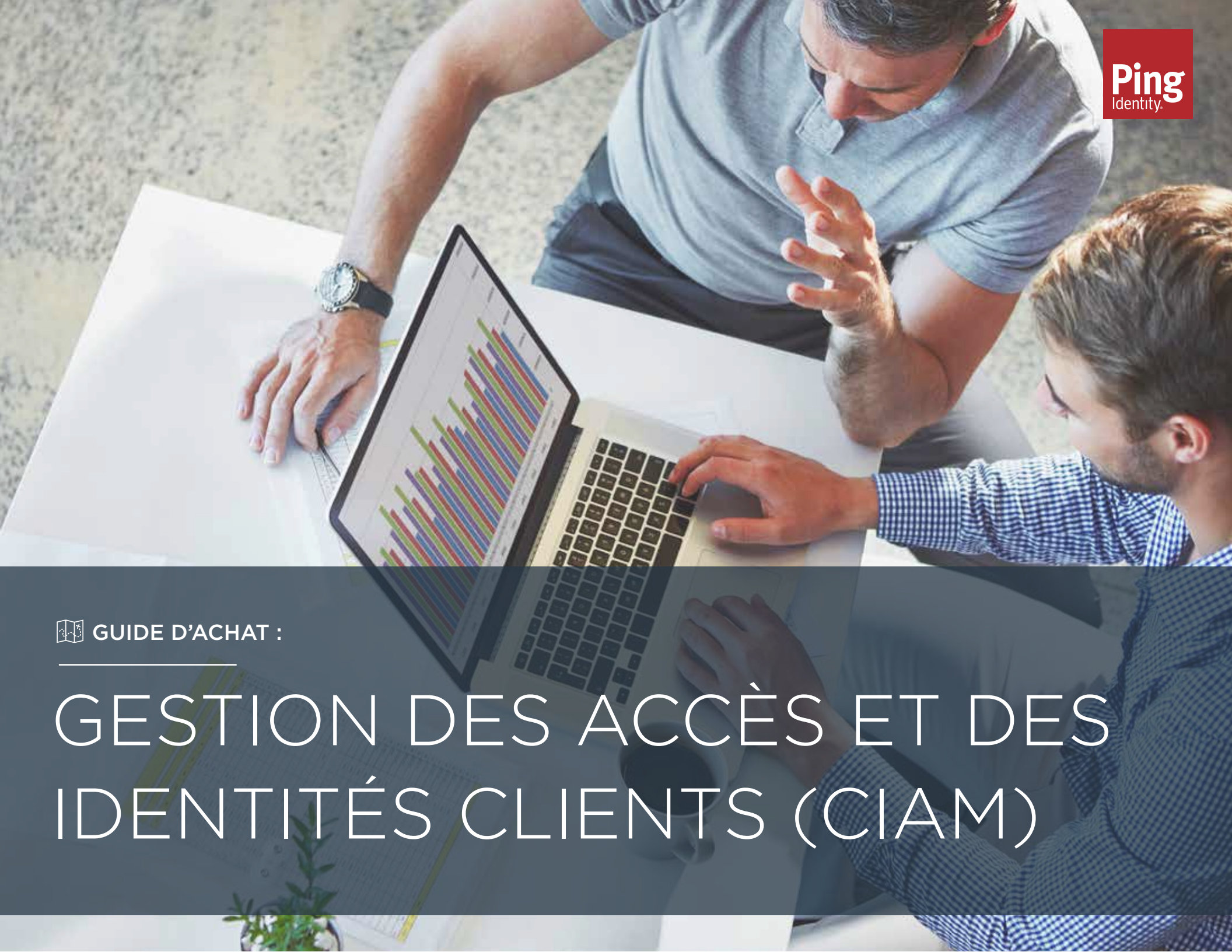


GUIDE D'ACHAT :

GESTION DES ACCÈS ET DES IDENTITÉS CLIENTS (CIAM)

UN MARCHÉ EN ÉVOLUTION

Au cours des dernières années, les exigences des entreprises qui gèrent les identités de leurs clients ont beaucoup changé. Cette évolution vient des analystes qui, en 2015, ont reconnu la gestion des accès et des identités clients (CIAM) comme étant un domaine distinct, avec ses propres exigences. Mais elle est également liée à un paysage concurrentiel plus rude où l'expérience client est le champ de bataille sur lequel se gagnent et se perdent les parts de marché.

Aujourd'hui, les clients sont hyperconnectés et adoptent de nouveaux schémas d'engagement qui divisent leur parcours sur de multiples canaux. Chaque interaction doit avoir une expérience client cohérente, être sécurisée et respecter la confidentialité des clients et les règles en matière de consentement.

Les moteurs d'activité CIAM concernent toutes les équipes, business, marketing, technique ou sécurité, et leurs exigences sont également très diverses. Pour trouver la solution CIAM appropriée, il faut une collaboration à tous les niveaux de l'entreprise et les diverses fonctionnalités d'une plate-forme CIAM complète.

DÉFINIR LA GESTION DES ACCÈS ET DES IDENTITÉS CLIENTS (CIAM)

Le nombre de solutions spécifiquement conçues pour répondre aux problématiques de gestion des accès et des identités clients a considérablement augmenté ces derniers temps. Ces solutions sont également de bien meilleure qualité. Le marché admet peu à peu qu'il est vain de considérer les identités clients comme une simple extension des solutions existantes de gestion des identités. La gestion des accès et des identités est fondamentalement différente pour les clients et pour les employés, pour plusieurs raisons :

1. **Moteurs d'activité** – Les moteurs d'activité de la gestion des accès et des identités sont, côté employés, la réduction des risques et l'amélioration des performances, et côté clients, l'amélioration de l'engagement client et l'augmentation du chiffre d'affaires.
2. **Échelle** – Les entreprises peuvent compter des dizaines de milliers d'employés pour les déploiements les plus importants, mais même les déploiements clients plus modestes peuvent compter des millions de clients et des milliards d'attributs.
3. **Inscription** – Les employés sont provisionnés et les RH guident le processus. Les clients s'inscrivent eux-mêmes.
4. **Confidentialité** – Les clients ont des règlements stricts en matière de confidentialité, par exemple le RGPD, que les employés n'ont pas. Toute infraction peut entraîner des préjudices pour la réputation de l'entreprise, une perte de confiance de la part des clients et de lourdes amendes.
5. **Exigences de niveau de service** – Si les exigences de niveau de service sont souvent élevées pour les employés, elles sont extrêmement élevées et encore plus importantes pour les clients. Ces derniers ne tolèrent aucun délai ni aucune interruption, alors que les employés ont peu de choix.

À leur niveau le plus basique, les solutions CIAM doivent fournir des fonctionnalités permettant de gérer trois aspects majeurs des interactions clients avec votre marque, notamment :

1. **Accès** – Les entreprises doivent être en mesure d'autoriser les clients à pénétrer sur leurs sites de manière sécurisée, via des fonctionnalités d'authentification et d'inscription. Ces fonctionnalités doivent être cohérentes sur les différents canaux et comporter des options permettant de rationaliser le processus, par exemple l'authentification sociale.
2. **Reconnaissance** – Les entreprises doivent être capables de reconnaître leurs clients une fois qu'ils sont authentifiés, quels que soient le canal ou l'application utilisés pour se connecter. Cela signifie autoriser les bons clients à accéder au contenu approprié et utiliser un profile unifié accessible à toutes les applications pour personnaliser les expériences clients sur les différents canaux.
3. **Protection** – Les entreprises doivent protéger leurs clients des failles et savoir bien gérer les données clients. Cela implique la mise en œuvre de bonnes pratiques d'authentification et d'inscription sécurisées, notamment l'authentification multi-facteurs (MFA) contextuelle, la sécurisation de la couche API/application avec contrôle d'accès et gestion de sessions, et la sécurisation des données clients via la gouvernance des accès, le chiffrement à chaque stade, etc.

Les entreprises doivent être en mesure de gérer ces catégories CIAM fondamentales avec une solution hautes performances, même à des échelles extrêmes.

DÉFINIR DES OBJECTIFS COMMERCIAUX

Définir vos objectifs commerciaux en amont vous permettra de centrer votre recherche et de vous assurer que vous envisagez des solutions adaptées. Pour une entreprise, les dix principales raisons pour l'acquisition d'une solution de gestion des accès et des identités clients sont :

1. **Transformation de l'entreprise numérique** – De plus en plus fréquemment, les entreprises adoptent des initiatives numériques visant à transformer la manière dont les clients interagissent avec leur marque. La gestion des accès et des identités autorise des expériences clients sécurisées, cohérentes et multicanal qui peuvent transformer la manière dont les entreprises mènent leurs activités numériques.
2. **Des menaces de sécurité croissantes** – Les fuites de données se produisent à une échelle et une fréquence plus importantes. Par conséquent, leur prévention devient une forte priorité pour les équipes informatiques et sécurité. Via une sécurité de bout en bout spécifiquement axée sur les identités clients, les solutions CIAM peuvent considérablement réduire le risque de fuites de données.
3. **Conformité aux règles de confidentialité** – Avec des règlements stricts en matière de confidentialité qui varient selon la région, le secteur, la société et même la personne concernée, il semble presque impossible de respecter les exigences de confidentialité des clients. Les solutions CIAM offrent des règles centralisées de gouvernance des accès aux données et d'autres fonctionnalités qui garantissent le respect du consentement des clients sur le partage de données, le stockage régional des données et autres exigences de confidentialité.
4. **Développement et fourniture d'applications mobiles** – Le lancement d'une nouvelle application peut souvent être le catalyseur d'une expérience client cohérente sur différents canaux. Cela peut permettre aux entreprises de poser les bases avant d'introduire échelle, performance, sécurité, single sign-on, authentification sociale et autres fonctionnalités CIAM.

Ces moteurs d'activité figurent parmi les plus fréquents, mais il peut en exister d'autres qui nécessitent échelle, performance, sécurité et autres fonctionnalités CIAM. Il peut s'agir par exemple de fusions/acquisitions, de l'adoption d'Internet des objets (IoT) ou autres.

LES TROIS MEILLEURES PRATIQUES POUR LA MISE EN ŒUVRE CIAM

1. **Équilibrer expérience client et sécurité** – Ceci nécessite une collaboration étroite entre les équipes business/marketing et les équipes IT et de sécurité IT. Cette collaboration va garantir le respect des exigences des équipes de sécurité ainsi que des standards de convivialité des équipes business.
2. **Ingénierie d'échelle** – L'accent est mis sur le nombre total d'utilisateurs mais aussi sur les scénarios de pics d'utilisation qui peuvent être parfois inattendus. Les interruptions de service lors de pics d'utilisation sont à l'origine des coûts les plus élevés. Assurez-vous que le prix de la solution que vous recherchez intègre l'utilisation des clients et répond à leur demande en terme de performance (des temps de réponse > à 1 seconde ne fonctionnent pas avec les applications grand public).
3. **Plan multicanal** – Que vous utilisiez le terme multicanal ou omnicanal, vos clients communiquent déjà avec votre entreprise via plusieurs canaux. Anticipez la manière dont votre solution CIAM va faciliter et conserver la cohérence lors des parcours clients multicanal.

PIÈGES À ÉVITER

1. Solutions partielles (par ex. MFA mais sans sécurité des couches de données, SSO mais sans unification des profils)
2. Un ensemble complexe et manquant de cohérence de différents logiciels pour répondre aux exigences CIAM
3. Projets « maison » qui semblent simples au premier abord mais qui finissent par coûter plus de temps et d'argent si l'on considère la sécurité, la confidentialité, l'authentification et la longue liste de bonnes pratiques associées.

LIGNES DIRECTRICES POUR SÉLECTIONNER UN ÉDITEUR DE SOLUTIONS CIAM

- Expérience et références
- Financièrement stable avec une place établie sur le marché
- Étendue des services / solution complète
  - Expérience dans la mise en place de solutions de gestions des identités
  - Expérience dans les services managés
- Mises en œuvre éprouvées avec échelle et performance extrêmes
- Sécurité de bout en bout pour les couches authentification, application/API et données
- Solutions basées sur des standards, extensibles et pérennes
- Possibilité de déploiement dans tout environnement (local, cloud, hybride)

CHECKLIST DES SOLUTIONS

CONSIDÉRATIONS FONCTIONNELLES

Exigences liées à la couche d'authentification

CRITÈRES D'ÉVALUATION	IMPORTANCE
L'éditeur propose-t-il des fonctionnalités de SSO fédéré ?	Le SSO fédéré garantit que les clients bénéficient d'une expérience d'authentification cohérente, avec identifiants communs, sur les différentes propriétés numériques.
L'éditeur fournit-il l'authentification sociale ?	Autoriser les clients à utiliser les identités existantes (comme Facebook ou Google) pour s'authentifier avec votre marque permet de rationaliser les expériences utilisateur lors de l'inscription et de l'authentification.
L'éditeur prend-il en charge la gestion des comptes en self-service ?	Une fois inscrits, les clients ont besoin de fonctionnalités en self-service pour gérer, ajouter, actualiser ou supprimer leurs propres données.
L'éditeur inclut-il les meilleures pratiques d'inscription comme la récupération des comptes et les règles de mots de passe à gestion centralisée ?	Il est important pour les éditeurs de solutions CIAM d'inclure les meilleures pratiques comme la réinitialisation du mot de passe et les règles de mots de passe à gestion centralisée afin d'améliorer la sécurité.
L'éditeur prend-il en charge l'authentification multi-facteurs contextuelle basée sur les risques ?	Exiger des utilisateurs qu'ils fournissent un second facteur d'authentification (par ex. SMS, biométrie) n'est pas une une option universelle. L'exigence du second facteur doit être basée sur les risques et dépendre du contexte de l'appareil de l'utilisateur, de sa géolocalisation ou du type de transaction qu'il effectue.

CONSIDÉRATIONS FONCTIONNELLES

Exigences liées à la couche application/API

CRITÈRES D'ÉVALUATION	IMPORTANCE
L'éditeur peut-il fournir un contrôle d'accès précis aux applications et aux API ?	Il est important de pouvoir centraliser la gestion du contrôle d'accès à des URL et API spécifiques. Les éditeurs doivent également fournir des règles centralisées et contextuelles de contrôle d'accès.
L'éditeur propose-t-il des fonctionnalités de gestion des préférences ?	Les entreprises doivent fournir aux clients la possibilité de définir explicitement les préférences, lesquelles doivent être stockées dans un profil client unifié afin de faciliter des expériences cohérentes et personnalisées sur les différents canaux.
L'éditeur fournit-il la gestion des sessions et la déconnexion unique ?	Les entreprises qui fournissent plusieurs canaux et applications ont besoin de pouvoir offrir la déconnexion unique pour toutes les applications afin d'améliorer sécurité et praticité pour les clients.

CONSIDÉRATIONS FONCTIONNELLES

Exigences liées à la couche de données

CRITÈRES D'ÉVALUATION	IMPORTANCE
L'éditeur propose-t-il une solution d'annuaire sécurisée et évolutive ?	Lors du stockage des données d'identité et de profil des clients, échelle et performance sont de la plus haute importance. Il est essentiel de garantir que les éditeurs fournissent un annuaire sécurisé et capable de stocker des millions d'identités et des milliards d'attributs. Assurez-vous qu'il existe des références client correspondant à l'échelle requise.
L'annuaire de l'éditeur 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. Il est important de pouvoir facilement stocker ces données dans votre annuaire client.

CONSIDÉRATIONS FONCTIONNELLES

Exigences liées à la couche de données

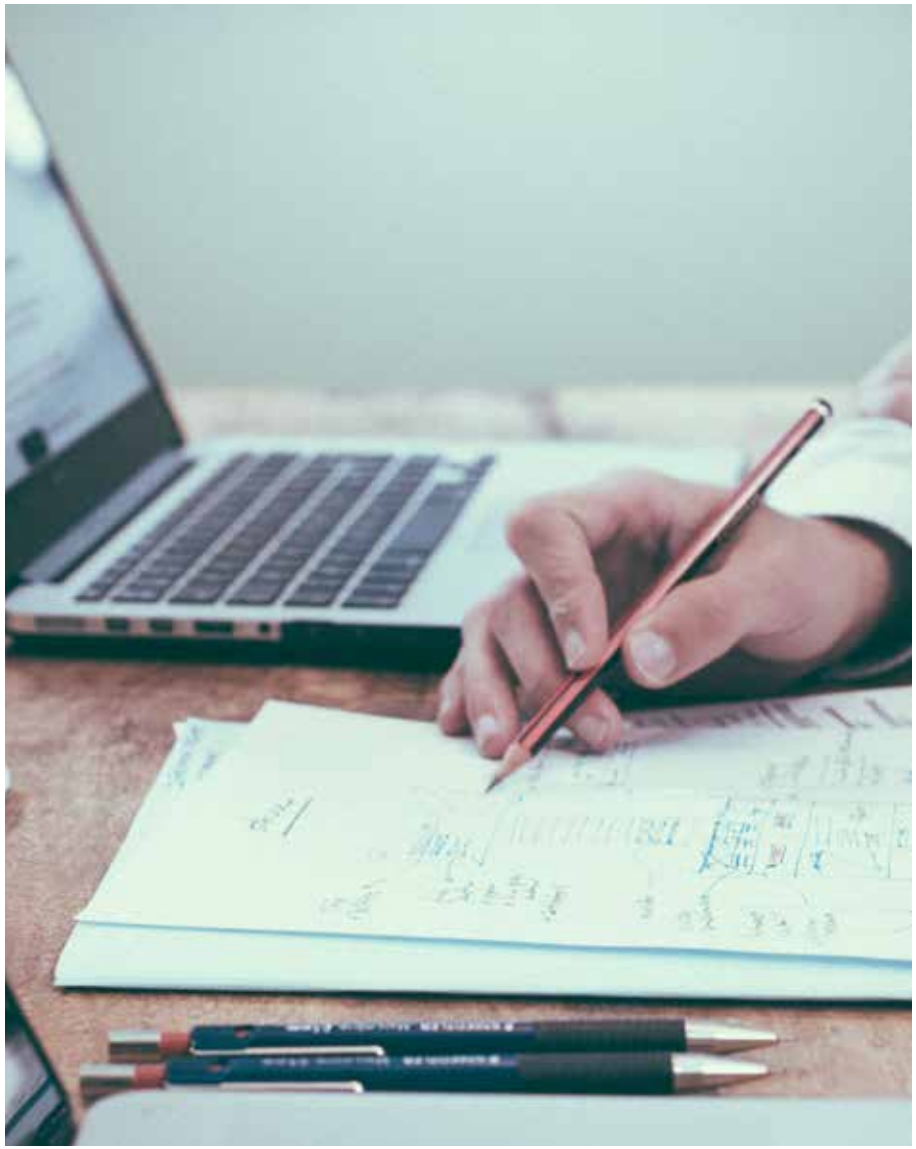
CRITÈRES D'ÉVALUATION	IMPORTANCE
L'annuaire de l'éditeur est-il accessible via des API REST ?	Les données client et les données de profil d'un annuaire doivent être accessibles via des API REST conviviales pour les développeurs afin d'en faciliter l'accès par les applications existantes et d'accélérer la mise sur le marché pour les nouvelles applications.
L'éditeur fournit-il des fonctionnalités de synchronisation des données bidirectionnelle en temps réel ?	La synchronisation des données bidirectionnelle en temps réel peut faciliter la création d'un profil client unifié (dans un annuaire CIAM) à partir de silos de données d'identité disparates, même s'il est nécessaire de gérer d'autres référentiels d'identités. Cela peut également faciliter les migrations de données sans aucun temps d'arrêt et sans aucun risque vers un annuaire client unifié.
L'éditeur prend-il en charge une gouvernance d'accès aux données précise dans le respect des règles de confidentialité ?	Les règles de confidentialité sont diverses et les exigences varient d'une personne à l'autre. Les solutions CIAM doivent contenir des règles à gestion centralisée appliquant le consentement du client et gouvernant le partage des données au niveau attribut-par-attribut pour toutes les applications internes et externes.
L'éditeur chiffre-t-il les données à chaque stade et met-il en œuvre d'autres bonnes pratiques de sécurité de la couche de données ?	Les fuites de données clients peuvent être un désastre pour la réputation de la marque. Il est donc important de garantir que les données clients sont chiffrées à chaque étape, au repos, en mouvement et en cours d'utilisation, et soumises à d'autres bonnes pratiques comme les alertes actives et passives et l'identification inviolable.

CONSIDÉRATIONS FONCTIONNELLES

Exigences liées à la plate-forme

CRITÈRES D'ÉVALUATION	IMPORTANCE
La plate-forme de l'éditeur repose-t-elle sur des standards ouverts ?	Il est important pour les plate-formes CIAM d'utiliser des standards ouverts comme SAML, SCIM, OAuth2 et OpenID Connect. Cela garantit l'extensibilité et la polyvalence de la solution CIAM.
L'éditeur prend-il en charge une sécurité forte de bout en bout sur chaque couche ?	Il est important que les éditeurs CIAM fournissent une sécurité forte au cours de l'authentification, au niveau de la couche application/API et de la couche de données.
L'éditeur peut-il gérer une échelle et une performance extrêmes et justifier de l'expérience correspondante ?	Les éditeurs doivent pouvoir prendre en charge des millions d'identités stockées et des milliards d'attributs, même pour les scénarios de pics d'utilisation avec des centaines de milliers d'utilisateurs simultanés. Ils doivent pouvoir justifier de 99,99999 % de disponibilité et d'une latence à la milliseconde.
L'éditeur propose-t-il des applications de référence personnalisables et des interfaces utilisateur prédéfinies ?	Presque toujours, les entreprises veulent entièrement personnaliser les interfaces utilisateur, mais les éditeurs qui fournissent ressources prédéfinies et interfaces permettent aux clients d'accélérer la mise sur le marché des nouvelles applications.

ÉVALUATION ET SÉLECTION DES ÉDITEURS



Après avoir défini toutes vos exigences, il convient de les organiser de manière à pouvoir facilement évaluer en quoi se démarque chaque éditeur. Une feuille de calcul fait très bien l'affaire. Créez des lignes pour chaque critère final, organisées selon les exigences clés des différents éléments, comme nous l'avons fait ci-dessus.

Ajoutez ensuite des colonnes pour chaque éditeur à évaluer. Évaluez chaque éditeur 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 = Réponse très limitée à l'exigence
2 = Répond partiellement à l'exigence
3 = Répond à l'exigence voire la surpasse

Avec ce système, vous évaluez chaque éditeur de 0 à 3 pour chacun de vos critères. Notez ensuite le total de chaque éditeur. L'éditeur possédant le meilleur score est également l'éditeur qui répond le mieux à vos exigences.

Vous voulez des conseils supplémentaires pour choisir la solution CIAM qui convient à votre entreprise ?
Lisez notre livre blanc : Une gestion des accès et des identités bien menée

#3061(rev) | 9.17 | v002