Livre blanc

Développer ou acheter ?

Faire le bon choix en matière d'identités clients

okta

Sommaire

2 Gérer les identités clients est une tâche complexe
8 Avantages de l'achat d'une solution CIAM
11 Conclusion
12 Comment Okta peut vous aider

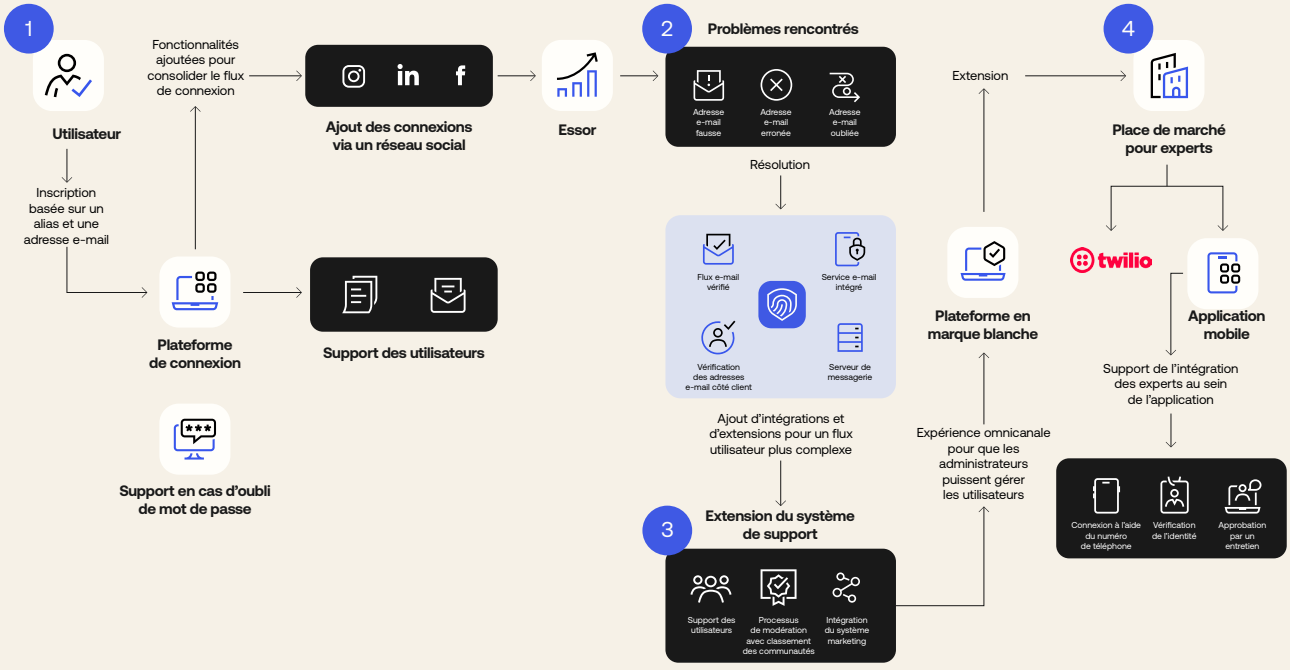
Gérer les identités clients est une tâche complexe

Chaque équipe chargée de développer une application web ou mobile est confrontée au même dilemme lorsqu'il s'agit d'intégrer de nouvelles fonctionnalités : les développer en interne ou utiliser des services prêts à l'emploi pour gagner du temps.

« Nos développeurs sont capables de gérer les identités clients. Après tout, ce n'est jamais qu'une boîte de dialogue de connexion. Ça n'a pas l'air très compliqué… »

Pourtant, la gestion des identités et des accès (CIAM, Customer Identity and Access Management) est bien plus qu'une simple boîte de dialogue de connexion. À mesure que l'entreprise se développe et ajoute des fonctionnalités, il est possible que la complexité de la gestion d'un système CIAM développé en interne monopolise plus de ressources que prévu. Le temps des développeurs est une ressource précieuse et les heures passées à maintenir les solutions « maison » en matière de gestion des identités, sécurité et respect de la confidentialité sont autant d'heures qu'ils ne consacrent pas à l'innovation liée au cœur de métier.

Concevoir une telle solution soi-même l'est encore plus…



Comment, dans ce cas, stimuler l'innovation et optimiser le temps des développeurs sans impacter la sécurité, les dates de lancement ou le budget ?

Une solution possible consiste à acquérir un système CIAM. S'appuyer sur une couche d'identité composée d'API, de kits SDK et de composants personnalisables prêts à l'emploi permet en effet d'écourter les délais de lancement, de réduire les coûts de développement et de permettre aux développeurs de se consacrer aux fonctionnalités centrales de l'application. Les applications orientées client ont toutes en commun un groupe de fonctionnalités essentielles en lien avec l'authentification, l'autorisation et la gestion des utilisateurs. Elles doivent en outre prendre en charge un certain nombre de workflows : création de comptes, connexion des utilisateurs, réinitialisation de mots de passe, récupération de comptes et inscription MFA, entre autres. Par ailleurs, les applications doivent prévoir des niveaux d'accès différents selon l'utilisateur.

Ce livre banc traite des principaux facteurs à prendre en compte au moment de choisir entre développement et achat, et décrit les avantages d'une solution préintégrée.

> « [Avec Okta] dans ma palette d'outils, je sais que nous allons progresser rapidement car la composante de l'identité est prise en charge. »
>
> **Scott Howitt**
> CISO, MGM Resorts International

Diminution du coût total du développement d'applications

La gestion des identités est l'une des disciplines où le risque de dépassement des coûts est le plus élevé, car la complexité des fonctionnalités et des systèmes est souvent sous-estimée et ne cesse d'évoluer. La création en interne introduit une plus grande incertitude dans l'équation et les coûts augmentent considérablement lorsque les équipes internes s'égarent dans la création de fonctions utilisateur sophistiquées ou découvrent que leurs impératifs ont évolué sous l'effet d'un contexte changeant. Si les équipes parviennent à tout livrer à temps, c'est au prix de coûteuses ressources contractuelles. En confiant la gestion des identités à un fournisseur de confiance, vous aidez l'équipe de développement à tenir les objectifs de votre projet sans dépassement du budget.

Exemple de réduction du coût total du développement d'applications[1]

3	x	6	x	200 000 $	x	90 %	=	270 000 $
Nb de développeurs		Calendrier de la solution d'identité en mois		Salaire complet		Amélioration		**Réduction du coût total de possession**

« Dans le domaine de l'identité, la situation change quasiment d'heure en heure, et nous avions besoin d'un partenaire technologique capable de suivre le rythme. »

Eash Sundaram
EVP Innovation, Chief Digital & Technology Officer, JetBlue Airways

[1] Calcul moyen, de type Google, de la valeur d'un ingénieur pour les entreprises où la technologie est la principale source de revenus. Nous calculons ici la contribution au chiffre d'affaires annuel moyen d'un ingénieur, multipliée par le nombre d'ingénieurs détachés de l'équipe ingénierie pour développer une couche d'identités.

Concentration des ressources sur les fonctionnalités de base de l'application

Votre réussite dépend de votre capacité à exécuter correctement les fonctionnalités essentielles qui rendent l'application utile à ceux qui s'en servent. Une couche de gestion des identités avancée libère votre équipe afin qu'elle puisse donner la priorité aux fonctionnalités qui génèrent des revenus et favorisent l'engagement client. Elle permet en outre aux développeurs de passer plus rapidement à la deuxième, troisième ou quatrième application attendue des clients.

Réduction du risque de sécurité et de non-conformité

À quand remonte la dernière mise à jour de votre algorithme de hachage des mots de passe ? Les données utilisateurs et les informations d'identification personnelle sont la cible privilégiée des attaques, alors que la durée de vie moyenne d'un algorithme de chiffrement efficace est de 18 mois seulement. La protection des utilisateurs est souvent délaissée au profit des impératifs d'augmentation du chiffre d'affaires ou de croissance. Un service de gestion des identités sécurisé suppose que votre équipe ait des connaissances (et du temps) pour corriger les vulnérabilités présentes dans chaque couche de l'infrastructure : système d'exploitation, bases de données, transport, applications, code, etc. Comme les équipes de développement possèdent rarement ce niveau d'expertise en matière de sécurité, elles n'apprennent l'échec de la protection des utilisateurs qu'une fois des données sensibles compromises. Par ailleurs, elles sont peu informées des événements touchant à la sécurité, comme le piratage d'un algorithme ou la découverte d'un vecteur d'attaque.

Un service de gestion des identités adapté protège les données de vos utilisateurs des cybercriminels, puisque l'équipe qui l'a conçu se compose d'experts spécialisés dans les techniques de protection avancée contre les attaques visant les identités et les accès. On peut citer par exemple un chiffrement performant, la sécurité des API, la protection avancée du pare-feu, des procédures efficaces de gestion des données et d'accès aux systèmes, etc. Ces mêmes mesures de sécurité et cette même infrastructure permettent à vos équipes de respecter les réglementations régionales et sectorielles, dont la loi HIPAA, le programme FedRAMP et le RGPD.

> « La Banque Nationale du Canada offre ses services à des millions de clients dans des centaines d'agences à travers le pays. Les objectifs de notre entreprise sont clairs, et l'un d'entre eux consiste à simplifier l'expérience client. Les fonctionnalités intelligentes d'authentification contextuelle d'Okta nous aident à offrir à nos clients une expérience en ligne à la fois fluide et sécurisée. »
>
> **Rish Tandon**
> CTO, Heal

Motivation des développeurs

Même si l'identité joue un rôle important dans la réussite d'une application orientée client, les développeurs rechignent souvent à créer une infrastructure de gestion des identités et de sécurité. Bien qu'il s'agisse d'une activité à haut risque et complexe, la gestion des utilisateurs est en effet perçue comme une opération banale, et les développeurs préfèrent se consacrer à des fonctionnalités en lien avec la différenciation des produits et les systèmes de pointe. La lourde charge de travail associée à l'implémentation de la sécurité utilisateur peut être particulièrement décourageante : les risques sont importants et les instructions, souvent contradictoires. À l'inverse, les développeurs jugent les services API REST-JSON modernes intéressants et accessibles.

Hauts niveaux d'évolutivité et de fiabilité
Lorsque la gestion des utilisateurs échoue, aucun accès n'est possible pour eux. Or, tout problème de disponibilité nuit à l'expérience de connexion des utilisateurs, et affecte leur perception de votre entreprise et de votre marque. La charge clients est impossible à prévoir, et les équipes marketing ne savent pas toujours à quel moment une promotion entraînera un afflux d'utilisateurs, ou ne communiquent pas toujours l'information. Si vous décidez de gérer vous-même cet aspect, vous devez être certain que l'équipe pourra offrir plusieurs niveaux de disponibilité, et monter en charge facilement en fonction de la base utilisateurs. Vous devez être prêt à assurer une double, voire une triple redondance au niveau de votre data center ou en vous associant avec un fournisseur de solutions IaaS (Infrastructure-as-a-Service). Vous devez prévoir des mises à jour et une maintenance transparentes pour offrir un service ininterrompu. Les entreprises qui assument ces responsabilités non négligeables jugent souvent le travail de maintenance écrasant. Un fournisseur de services de gestion des utilisateurs extérieur peut éliminer complètement ce casse-tête opérationnel.

> « Faciliter l'intégration à tous les niveaux de l'écosystème, assurer une gestion des identités commune à tous les systèmes et faire en sorte qu'elle soit au cœur de notre relation avec le client, avec une fiabilité et une disponibilité élevées : voilà ce qui comptait vraiment à nos yeux. »
>
> **James Fairweather**
> Senior Vice President of E-Commerce and Technology, Pitney

Avantages de l'achat d'une solution CIAM

Il existe d'excellentes raisons d'acheter une solution de gestion des identités plutôt que la développer :

Augmentation du chiffre d'affaires grâce à des délais de lancement de lancement d'applications accélérés
Les besoins des clients peuvent changer brusquement et les entreprises d'aujourd'hui doivent être suffisamment agiles pour profiter des opportunités offertes par le marché, sans quoi elles risquent de mettre en péril leurs revenus. Une solution CIAM adaptée peut offrir une couche d'identité permettant de sécuriser l'expérience client. Ainsi, les équipes de développement n'ont pas à réinventer la roue pour ce qui est de la gestion des authentifications, autorisations et utilisateurs, ce qui leur permet de se concentrer sur les fonctionnalités différenciant votre application et de les proposer aux consommateurs. Comme il s'agit autant de préserver le chiffre d'affaires que de le faire progresser, l'évolutivité a également son importance. Certaines actions mobilisant d'importantes ressources, par exemple l'authentification, le chiffrement des mots de passe et la recherche, doivent s'adapter à la demande utilisateur pendant les pics d'activité.

Diminution des coûts d'ingénierie
L'implémentation d'une solution CIAM d'un éditeur tiers est simple, et l'activation de fonctionnalités puissantes est généralement immédiate. Vous pouvez ainsi réaffecter des centaines, voire des milliers d'heures de développement à l'écriture de la logique métier, au lieu de les consacrer à la conception d'une solution d'authentification. Le temps alloué aux tests et à la sécurité des processus d'authentification peut être réinvesti dans le développement d'applications essentielles. L'intégration et le mappage des fournisseurs d'identité peuvent être longs et fastidieux. Avec la solution tierce adaptée, ces intégrations sont déjà préconfigurées et rapides à implémenter. Une solution CIAM prête à l'emploi doit également intégrer des kits SDK destinés aux infrastructures de développement courantes, ce qui réduit encore le codage nécessaire à l'intégration du système d'authentification. L'équipe d'ingénierie d'une société peut se concentrer sur la configuration au lieu du codage et de la personnalisation.

Sécurité renforcée
À quand remonte la dernière mise à jour de votre algorithme de hachage des mots de passe ? Les données utilisateurs et les informations d'identification personnelle sont la cible privilégiée des attaques. La durée de vie moyenne d'un algorithme de chiffrement efficace est de 18 mois seulement, mais la protection des utilisateurs est souvent délaissée au profit des impératifs d'augmentation du chiffre d'affaires ou de croissance. Une solution CIAM prendra en charge certaines responsabilités telles que la sécurité du stockage et du transport des données utilisateur, ou le respect des certifications et politiques de conformité locales ou nationales. Elle offre en outre des fonctions de fédération des identités, ce qui permet d'éviter certaines mauvaises pratiques de la part des utilisateurs, par exemple la réutilisation du même mot de passe pour éviter de mémoriser plusieurs identifiants de connexion.

Études de cas dans différents secteurs

Schneider Electric - Booster la croissance avec une gestion unifiée des identités

Comptant plus de 170 000 collaborateurs dans plus de 100 pays, Schneider Electric, un des leaders mondiaux de l'automatisation et de la gestion de l'énergie, avait besoin d'une stratégie de gestion des identités capable d'accompagner la prochaine phase de croissance de la société tout en optimisant l'utilisation des ressources. Lors du choix d'une solution CIAM, la première exigence de Schneider Electric était un système d'authentification unique (SSO) pour créer un processus d'authentification unifié. L'objectif était de pouvoir utiliser les mêmes identités et identifiants pour l'ensemble des systèmes et applications de l'entreprise.

Une analyse de rentabilité a rapidement démontré qu'il était plus avantageux pour Schneider d'affecter ses ressources humaines à la réalisation des objectifs et impératifs métier essentiels. Une solution de gestion des identités tierce lui permettait de surmonter les obstacles au sein du groupe et de résoudre la problématique de l'intégration des identités. Okta Customer Identity Cloud (anciennement Auth0) offrait aussi une solution robuste et flexible, orientée développeur et facile à intégrer. Adaptée aux environnements web et mobile, la plateforme prend en charge des normes ouvertes et propose des fonctionnalités robustes et évolutives, doublées d'une prise en charge étendue de fournisseurs d'identité et d'un processus de migration simple.

Une fois Okta Customer Identity Cloud sélectionné et implémenté, la société a pu bénéficier de ses nombreux avantages. La solution de gestion des identités a permis de supprimer les tâches de développement dans ce domaine, libérant ainsi davantage de ressources pour l'innovation IT. Elle a réduit les délais de lancement, renforcé la sécurité et favorisé l'application de bonnes pratiques. Okta Customer Identity Cloud a également permis de réagir plus rapidement à l'apparition de nouvelles vulnérabilités.

« Avant que n'importe quel site d'information ne signale la vulnérabilité jour zéro Heartbleed, Auth0 [à présent Okta Customer Identity Cloud], nous a envoyé un e-mail pour nous avertir de la situation. Il existait déjà un correctif pour éliminer la menace Heartbleed des systèmes Auth0. L'e-mail de confirmation qui a suivi confirmait qu'Auth0 avait déjà installé ledit correctif sur l'instance du service Auth0 de Schneider Electric.

Auth0 a réellement facilité la tâche de l'équipe responsable de la plateforme. Non seulement le problème de sécurité a été corrigé, mais notre équipe IT a pu gagner un temps précieux en tirant parti des instructions détaillées communiquées pour corriger les problèmes et en faire part à notre équipe interne. Qui plus est, Auth0 a renouvelé les certificats, une tâche qui aurait demandé beaucoup de temps à notre équipe.

Grâce à la plateforme Auth0, nous pouvons planifier et intégrer l'architecture d'identités à un stade précoce pour gagner un temps précieux et garantir la mise en place d'un système sécurisé au démarrage d'un projet. »

Stephen Berard
Schneider Electric

Bluetooth — Unification des identités dans toutes les applications on-premise et cloud

Bluetooth, leader mondial des technologies sans fil, possédait un écosystème en constante expansion qui présentait plusieurs défis. L'activité, qui avait débuté sous la forme d'une seule application, s'est rapidement développée et déclinée en un large éventail d'applications différentes. Les applications développées en interne ainsi que les solutions SaaS d'éditeurs tiers (SharePoint, ServiceNow, SiteCore) nécessitaient toutes des identifiants d'authentification différents. La solution propriétaire existante de Bluetooth était basée sur les formulaires et utilisait des identifiants de type nom d'utilisateur / mot de passe. Une telle plateforme n'était pas adaptée à l'identité fédérée. La société nécessitait une solution d'identité moderne avec une authentification unique pour toutes ses applications « maison » et SaaS externes. La solution devait être implémentée sans interrompre le fonctionnement de la plateforme existante et proposer un calendrier de migration complète. Les rôles et accès utilisateur étaient également essentiels pour garantir le niveau d'accès adapté aux documents confidentiels.

Une solution d'identité répondait à ces exigences. Facile à implémenter, elle a permis à l'équipe d'ajouter des fonctionnalités SSO et une solution d'authentification moderne. L'ancien système a été maintenu en place pendant l'implémentation et l'exécution du plan de migration. L'implémentation n'a pris que quelques jours, et non les mois habituellement nécessaires à la mise en place d'une plateforme interne. Une documentation de premier ordre avec des échantillons de code détaillés couvrait un large éventail de thèmes, des plus élémentaires aux plus avancés, ce qui a permis aux ingénieurs SIG de Bluetooth de comprendre et d'implémenter rapidement leur solution d'identité moderne. Bluetooth a collaboré avec une équipe de Developer Success Engineers pour mettre au point une preuve de concept afin de présenter conjointement les fonctionnalités de la plateforme. Les délais de réponse du support étaient courts avec une exécution rapide.

Conclusion

L'innovation sans compromis

La gestion des identités moderne s'accompagne de nombreux défis. S'adapter sans cesse à l'évolution des normes et des bonnes pratiques, et corriger continuellement les bugs de sécurité réduisent le temps et l'argent à consacrer au cœur de métier. En optant pour des fonctionnalités évolutives, capables de s'adapter aux besoins changeants de votre entreprise et en comprenant comment d'autres sociétés ont correctement évalué et implémenté leurs propres solutions, vous pouvez exploiter pleinement les avantages d'une solution de gestion des identités sans nuire à la sécurité et à l'expérience utilisateur, ni devoir augmenter les heures développeur.

Plutôt que de constituer un point de risque et un frein potentiel aux activités, la gestion des identités peut se transformer en un système qui renforce la capacité de votre entreprise à booster ses revenus. Avec Okta Customer Identity Cloud, vous pouvez implémenter un CIAM en quelques jours et non plusieurs mois, et pérenniser votre activité en utilisant une solution CIAM simple, complète et extensible. With Okta Customer Identity Cloud, you can implement CIAM in days instead of months, future-proofing your organisation by utilising the easiest, most comprehensive and extensible CIAM solution available.

Comment Okta peut vous aider

Okta peut vous aider à gérer les identités de vos utilisateurs. En tant qu'experts en sécurité, nous avons conçu une plateforme IDaaS (Identity-as-a-Service) conçue pour offrir une sécurité de pointe. Plus de 80 000 développeurs dans 167 pays ont choisi Okta Customer Identity Cloud comme solution de gestion des identités.

Fonctionnalités et avantages :

- Possibilité de configurer et d'implémenter une solution de fédération pour entreprise et une authentification unique (SSO) qui ne nécessite aucun codage et une configuration minimale
- Connecteurs pour solutions d'entreprise dont Active Directory, LDAP, ADFS, SAML, Google Apps, etc.
- Connexions aux principaux réseaux sociaux, dont LinkedIn, Facebook, Twitter, Google, et bien d'autres
- Authentification classique (nom d'utilisateur et mot de passe) via la base de données Auth0 ou toute autre base de données personnalisée, alliée à des fonctionnalités de sécurité améliorées telles que l'authentification multifacteur (MFA), la détection de mots de passe compromis, la protection contre les attaques par force brute et la détection des anomalies
- Migration simple des utilisateurs depuis les systèmes existants, sans réinitialisation forcée des mots de passe
- Méthodes destinées à auditer et à consulter des analyses basées sur l'identité afin de garantir la conformité et de multiplier les opportunités de ventes additionnelles
- Gestion aisée de l'accès utilisateur grâce à des autorisations granulaires et à de puissantes règles personnalisées
- Délégation de l'administration pour permettre d'accorder à des utilisateurs ou groupes spécifiques un contrôle granulaire permettant l'accès, la visibilité et la gestion des utilisateurs
- Avec Okta Customer Identity Cloud, il faut moins de 30 minutes au développeur pour configurer une solution de gestion des identités robuste et personnalisable pour n'importe quelle pile technologique

Ressources

Pour d'autres témoignages de sociétés ayant évalué Okta Customer Identity Cloud (Auth0), consultez notre page Clients, notre page Tarifs ou contactez notre service commercial.