

Une publication:

okta

L'identité client

pour
les nuls[®]
A Wiley Brand



L'importance de
l'identité client

Les atouts d'une identité
client avancée

Bonnes pratiques
de l'identité client

Édition spéciale Okta

Lawrence C. Miller
Jeremie Certes

À propos d'Okta

Partenaire leader indépendant en matière d'identité, Okta permet à chacun d'utiliser en toute sécurité n'importe quelle technologie, partout, sur n'importe quel terminal ou application. Nos solutions Workforce Identity Cloud et Customer Identity Cloud permettent un accès, une authentification et une automatisation sécurisés et flexibles, qui transforment la manière dont nous évoluons au sein du monde numérique et qui placent l'identité au cœur de la sécurité et de la croissance de l'entreprise.



L'identité client

Édition spéciale Okta

**by Lawrence C. Miller
et Jeremie Certes**

pour
les nuls[®]
A Wiley Brand

L'identité client pour les nuls®, Édition spéciale Okta

Publié par
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774 États-Unis
www.wiley.com

Copyright © 2024 de John Wiley & Sons, Inc., Hoboken, New Jersey

Aucune partie de cet ouvrage ne peut être reproduite, conservée dans un système d'extraction, ou transmise sous quelque forme ou par quelque moyen que ce soit, par voie électronique ou mécanique, photocopie, enregistrement, numérisation ou autre, sans l'accord écrit préalable de l'éditeur, sauf si les articles 107 et 108 de la loi des États-Unis de 1976 relative au copyright (« United States Copyright Act ») l'autorisent. Les demandes d'autorisation auprès de l'éditeur doivent être adressées à Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 7486011, fax (201) 7486008, ou en ligne à l'adresse <http://www.wiley.com/go/permissions>.

Marques commerciales: Wiley, Pour les nuls, le logo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier et les appellations commerciales afférentes sont des marques de commerce ou des marques déposées de John Wiley & Sons, Inc. et/ou de ses sociétés affiliées aux États-Unis et dans d'autres pays, et ne peuvent pas être utilisées sans autorisation écrite. Les autres marques citées sont la propriété de leurs détenteurs respectifs. John Wiley & Sons, Inc. n'est associé à aucun produit ou distributeur mentionné dans cet ouvrage.

EXCLUSION DE GARANTIE ET LIMITATION DE RESPONSABILITÉ : TANDIS QUE L'ÉDITEUR ET LES AUTEURS ONT FOURNI TOUS LES EFFORTS POSSIBLES DANS LA PRÉPARATION DE CET OUVRAGE, ILS NE FONT AUCUNE DÉCLARATION NI N'ACCORDENT AUCUNE GARANTIE QUANT À L'EXACTITUDE OU À L'EXHAUSTIVITÉ DU CONTENU DU PRÉSENT OUVRAGE ; ILS REJETTENT SPÉCIFIQUEMENT TOUTES LES GARANTIES, Y COMPRIS, SANS AUCUNE LIMITE, LES GARANTIES DE QUALITÉ MARCHANDE OU D'ADÉQUATION À UN USAGE PARTICULIER. AUCUNE GARANTIE NE PEUT ÊTRE CRÉÉE OU PROROGÉE PAR DES REPRÉSENTANTS COMMERCIAUX, DES SUPPORTS DE VENTE ÉCRITS OU DES ANNONCES PROMOTIONNELLES POUR CET OUVRAGE. LA MENTION D'UNE ORGANISATION, D'UN SITE INTERNET OU D'UN PRODUIT DANS LE PRÉSENT OUVRAGE, EN CITATION ET/OU COMME SOURCE POTENTIELLE D'INFORMATIONS SUPPLÉMENTAIRES NE SIGNIFIE PAS QUE L'ÉDITEUR OU LES AUTEURS ENTÉRINENT LES INFORMATIONS OU LES SERVICES QUE PEUT FOURNIR OU RECOMMANDER L'ORGANISATION, LE SITE INTERNET OU LE PRODUIT EN QUESTION. LE PRÉSENT OUVRAGE EST VENDU ÉTANT ENTENDU QUE L'ÉDITEUR N'OFFRE PAS DE SERVICES PROFESSIONNELS. LES CONSEILS ET STRATÉGIES QU'IL CONTIENT PEUVENT NE PAS CONVENIR À TOUTES LES SITUATIONS. SI NÉCESSAIRE, CONSULTEZ UN SPÉCIALISTE. LES LECTEURS DOIVENT PAR AILLEURS SAVOIR QUE LES SITES INTERNET MENTIONNÉS DANS LE PRÉSENT OUVRAGE PEUVENT AVOIR CHANGÉ DEPUIS LE MOMENT OÙ L'OUVRAGE A ÉTÉ RÉDIGÉ. NI L'ÉDITEUR, NI LES AUTEURS NE SERONT TENUS RESPONSABLES DE TOUTE PERTE DE PROFITS OU D'AUTRES DOMMAGES COMMERCIAUX, Y COMPRIS, MAIS SANS S'Y LIMITER, LES DOMMAGES SPÉCIAUX, ACCESSOIRES, CONSÉQUENTIFS OU AUTRES.

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un guide *Pour les nuls* destiné à votre entreprise ou organisation, veuillez contacter notre service de développement commercial aux États-Unis, par téléphone au +1 877 409 4177, par e-mail à info@dummies.biz, ou consulter notre site www.wiley.com/go/custompub. Pour obtenir des informations sur les licences relatives à la marque *Pour les nuls* pour des produits et services, contactez BrandedRights&Licenses@wiley.com.

ISBN 978-1-394-22821-8 (livre broché) ; ISBN 978-1-394-22822-5 (eBook)

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation de :

Rédactrice projet : Rachael Chilvers

Représentante du développement commercial : Molly Daughy

Directrice des acquisitions :
Traci Martin

Éditeur de production :

Directeur éditorial : Rev Mengle

Saikarthick Kumarasamy

Introduction

Il y a fort à parier que vous avez déjà utilisé l'identité client dans votre vie personnelle en qualité de client d'une marque – peut-être sans en avoir conscience. Ainsi, vous avez certainement déjà créé un compte sur un site web pour acheter des billets de concert, ou utilisé l'un de vos comptes de réseaux sociaux pour vous connecter à un nouveau site d'e-commerce. Vous avez probablement réalisé des transactions bancaires sur votre smartphone après avoir reçu un code à usage unique par SMS pour valider votre identité. Ce ne sont là que quelques exemples de la façon dont les clients utilisent l'identité client au quotidien sur leurs applications, sites web et portails préférés.

Dans ce guide, vous découvrirez comment une solution d'identité client peut aider votre entreprise à offrir une expérience client numérique fluide et sécurisée à chaque utilisateur.

À propos de ce livre

L'identité client pour les nuls, Édition spéciale Okta, comporte huit chapitres qui explorent les questions suivantes :

- » **Les principes fondamentaux de l'identité client (chapitre 1)**
- » **Pourquoi l'identité client est plus importante que jamais (chapitre 2)**
- » **Pourquoi il n'est pas recommandé de développer une solution d'identité client en interne (chapitre 3)**
- » **En quoi consiste une solution d'identité client et comment elle peut aider votre entreprise (chapitre 4)**
- » **Les fonctionnalités incontournables d'une solution d'identité client (chapitre 5)**
- » **Les atouts d'une solution d'identité client adaptée à vos besoins métier (chapitre 6)**
- » **Le futur de l'identité client (chapitre 7)**
- » **Dix considérations liées à l'identité client qui sont gage de réussite (chapitre 8)**

Chaque chapitre est rédigé comme un tout, indépendant du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc vous y référer directement. Vous pouvez lire le guide dans l'ordre qui vous convient (même si nous déconseillons de le lire à l'envers).

Quelques suppositions

Même s'il ne faut préjuger de rien, en théorie, nous partons cependant des quelques présupposés suivants.

Ainsi, nous supposons que vous occupez un poste où vous êtes responsable de créer, faire évoluer, moderniser, intégrer, organiser et/ou sécuriser l'application, le site web ou le portail destiné à vos clients ou partenaires. Vous êtes peut-être développeur ou architecte d'applications, chef de produit, responsable ingénierie, responsable numérique, directeur technique, directeur des systèmes d'information (DSI), directeur de la sécurité des systèmes d'information (DSSI), directeur produit, directeur marketing ou tout autre intervenant spécialisé dans ou concerné au premier chef par l'identité client.

Les icônes utilisées dans ce livre

Ce livre est émaillé de différentes icônes destinées à attirer l'attention du lecteur sur des informations importantes. En voici le détail :



RAPPEL

Cette icône signale des informations importantes à retenir – ou, si vous nous permettez l'analogie, à inscrire dans votre mémoire non volatile.



TECHNIQUE

Si le jargon et les explications techniques vous enchantent, vous serez au paradis. Cette icône signale les informations un peu plus pointues que ne manqueront pas d'apprécier tous les technophiles.



CONSEIL

Un petit conseil est toujours le bienvenu : nous espérons que vous apprécierez ces informations utiles.



AVERTISSEMENT

Cette mention signale des écueils potentiels.

Voir plus loin que le livre

Ce guide ne peut malheureusement pas être exhaustif. Si vous souhaitez en savoir plus, rendez-vous sur le site <https://www.okta.com/fr/customer-identity>.

- » Définition de la gestion des identités et des accès clients (CIAM)
- » Impact d'une expérience d'identité client médiocre sur l'expérience client
- » Comment améliorer l'expérience utilisateur sur les applications mobiles, sites web et portails au moyen de l'identité client
- » Principales fonctionnalités de l'identité client

Chapitre 1

Qu'est-ce que l'identité client ?

Noms d'utilisateur et mots de passe font désormais partie de notre vie quotidienne. Les consommateurs ont pris l'habitude de gérer une multitude de comptes, qu'il s'agisse d'acheter en ligne, d'effectuer des transactions bancaires ou d'utiliser des applications mobiles. Toutes ces pratiques sont basées sur la gestion des identités et des accès clients (CIAM, Customer Identity and Access Management). En réalité, sans doute sans vous en rendre compte, vous faites déjà la différence entre une bonne et une mauvaise expérience d'identité client. Ainsi, il est probable que votre application de banque en ligne vous semble digne de confiance et facile d'emploi dès lors où elle vous permet de vous authentifier par empreinte digitale ou reconnaissance faciale. À l'inverse, vous avez certainement déjà abandonné un panier d'achat en ligne lorsque vous trouviez la procédure d'enregistrement trop longue et fastidieuse. Il faut avouer que sur certains sites, on passe plus de temps à remplir des formulaires qu'à trouver les articles dont on a besoin.

Ce chapitre explore les principes fondamentaux de l'identité client, tels que son fonctionnement, les effets négatifs d'une expérience d'identité client médiocre sur la confiance, l'importance de l'identité client pour vos clients et applications, ainsi que les fonctionnalités que toute solution d'identité client doit posséder.

Définition de l'identité client

Même si le terme lui-même ne vous est pas familier, vous utilisez l'identité client au quotidien : lorsque vous accédez à des applications mobiles, que vous vous inscrivez à un nouveau service en ligne ou que vous vous authentifiez sur votre site préféré. L'identité client offre une couche d'identité numérique qui peut s'intégrer aux applications, sites web et portails orientés clients. C'est elle qui vous permet d'identifier vos clients et les contenus auxquels ils accèdent lorsqu'ils utilisent vos services (applications, portails, sites web, etc.), où qu'ils se trouvent dans le monde et quel que soit le terminal qu'ils emploient. Cependant, l'identité client ne sert pas uniquement à la connexion et à l'authentification des utilisateurs, mais elle intervient également dans le processus d'enregistrement et de création de comptes, c'est-à-dire à chaque étape du parcours client.

Pour cette raison, une expérience d'identité client médiocre peut faire fuir les consommateurs au profit de concurrents qui offrent des expériences plus fluides et intuitives. Mais comment définit-on la bonne ou mauvaise qualité d'une expérience d'identité client ?

Évaluation de la qualité de l'identité client

La capacité à sécuriser les données et les accès est un aspect crucial de l'expérience que vous offrez à vos clients. Toutefois, cet effort de sécurisation sera vain si le parcours client est pénible et nuit à l'engagement. Il est probable que vous ayez déjà vécu une mauvaise expérience client dans vos transactions personnelles et professionnelles. Voici quelques exemples de points de friction liés à l'identité client, c'est-à-dire de situations qui obligent les clients à :

- » Créer un compte et un mot de passe juste pour consulter un site web
- » Créer plusieurs comptes et mots de passe pour accéder aux applications, sites web et portails d'une même entreprise
- » Utiliser différents comptes et mots de passe pour accéder aux services d'une même entreprise
- » Devoir fournir une multitude d'informations personnelles au cours d'une procédure d'enregistrement interminable, juste pour créer un compte

- » S'adapter à différentes procédures de connexion et fonctionnalités selon le terminal utilisé
- » Appeler le service client pour réinitialiser un mot de passe oublié ou incorrect
- » Saisir un code SMS en plus d'un mot de passe à chaque connexion, même s'ils se connectent toujours depuis le même lieu et le même terminal

En revanche, une bonne expérience d'identité client offre de nombreux avantages :

- » Procédure d'enregistrement et de création de compte simple et rapide, n'exigeant que les informations strictement nécessaires
- » Reconnaissance faciale sur les terminaux intelligents (fini les mots de passe !)
- » Validation par SMS ou e-mail pour les transactions financières sensibles, pour se sentir plus en sécurité
- » Accès à tous les services d'une entreprise via le même compte

Lorsque l'identité client est mal gérée, le parcours client est entravé par des points de friction inutiles, comme un processus d'enregistrement trop long et intrusif, ou la nécessité d'appeler un service client pour réinitialiser un mot de passe. De plus, vos développeurs doivent créer des intégrations et des connexions personnalisées pour vos nouvelles applications, ce qui ralentit leur lancement. Les clients doivent créer des comptes distincts pour chaque application, site web et portail de l'environnement numérique d'une entreprise ; en parallèle, les administrateurs doivent gérer ces comptes dans des annuaires séparés. Enfin, une identité client médiocre n'offre pas la fiabilité et l'évolutivité dont les entreprises agiles ont besoin dans notre économie numérique.



CONSEIL

Ne laissez pas les points de contact de votre identité client devenir des points de tension. Faites de l'identité client le point de départ d'une expérience optimale, qui satisfera vos clients de bout en bout.

Types de clients, de modèles de vente et d'applications

Pour offrir une expérience client omnicanale fluide sur tous vos produits et services, à tout moment et à tous les points d'interaction, adoptez une solution d'identité client avancée. L'identité est la première étape du parcours client pour de nombreux sites web, applications et portails, et elle influencera la totalité de l'expérience client.

Que votre clientèle soit composée de particuliers, d'entreprises ou d'un mélange des deux, votre solution d'identité client doit tout prendre en charge, ce qui signifie être compatible avec des modèles de vente variés : B2C (business-to-consumer), B2B (business-to-business) et B2B2C (business-to-business-to-consumer).

En outre, les divers types de clients privilégieront probablement des canaux différents dans leurs interactions avec votre entreprise. Par exemple, les particuliers préféreront utiliser votre application mobile, tandis que vos partenaires se serviront davantage de leur ordinateur de bureau. Votre solution doit donc tenir compte de tous ces paramètres : types de clients, canaux préférés et terminaux généralement utilisés.

Par ailleurs, dans les contextes B2B et B2B2C, vous devrez certainement prévoir des connexions et des intégrations sécurisées aux applications et portails de vos partenaires. De même, vous devrez sans doute fédérer leurs identités à l'aide de services d'annuaire tels qu'Active Directory et LDAP (Lightweight Directory Access Protocol).

Enfin, il est possible que vos clients aient besoin d'accéder à vos services à la fois sur vos applications mobiles, vos sites web et vos portails. Dans ce cas, leur expérience doit être uniforme sur tous les types d'applications et les fonctionnalités doivent être accessibles de façon fluide.

Principales fonctionnalités

Les trois principales fonctionnalités d'une solution d'identité client efficace sont l'authentification, l'autorisation et la gestion des utilisateurs. Dans ce cadre, les utilisateurs sont vos clients et vos partenaires.

Une authentification appropriée permet de garantir que les utilisateurs se connectant à leur compte sont bien qui ils prétendent être. Cette fonctionnalité empêche les cybercriminels d'accéder aux données sensibles (informations bancaires, adresses, numéros de sécurité sociale, etc.) ou de réaliser des transactions frauduleuses (par exemple un transfert d'argent depuis un compte en banque).

Un processus efficace d'autorisation permet de vérifier qu'un utilisateur possède le bon niveau d'accès à une application et/ou à une ressource.

Enfin, une gestion des utilisateurs transparente permet aux administrateurs de mettre à jour les autorisations d'accès et d'implémenter des politiques de sécurité, ce qui favorise la fluidité et la sécurité des expériences clients.

- » Offrir aux clients une expérience optimale
- » La confiance, pierre angulaire de la relation client
- » Permettre et accompagner la transformation digitale

Chapitre 2

Pourquoi l'identité client est plus importante que jamais

De nos jours, les clients attendent et exigent une expérience fluide et personnalisée à chaque interaction avec une marque. Les entreprises qui ne parviennent pas à répondre à cette demande seront incapables d'attirer de nouveaux clients ou de fidéliser leur clientèle existante.

Autre élément non négociable : gagner leur confiance. Une entreprise qui n'arrive pas à assurer la sécurité et la confidentialité des informations personnelles perdra des clients — y compris ceux qui ne sont pas directement affectés, mais qui retirent leur confiance à une marque victime d'une compromission.

Dans un tel contexte, la transformation digitale n'est plus seulement un projet, mais devient une obligation. Pour survivre et prospérer dans notre économie moderne, résolument numérique, chaque entreprise, quel que soit son secteur, doit intégrer la technologie dans ses activités.

Ce chapitre explique comment l'expérience client, la sécurité, la confidentialité et la transformation digitale sont autant de facteurs qui motivent et accélèrent tout à la fois la nécessité de déployer une solution d'identité client de pointe, maintenant plus que jamais.

Répondre à la demande en matière d'expérience client

L'expérience client aujourd'hui doit être fluide, personnalisée et omnicanale. Cette exigence implique d'offrir à vos clients un accès sans points de friction, quand ils le veulent et d'un simple geste aux produits, services, informations et autres ressources dont ils ont besoin sur leur appareil préféré : terminal intelligent, ordinateur, tablette ou smartphone.

Il n'y a pas si longtemps, les consommateurs réalisaient presque tous leurs achats dans des magasins physiques, et regardaient des films au cinéma ou à la télévision à la date et à l'heure où ils étaient programmés. Puis, ils ont commencé à interagir avec les entreprises sur leur ordinateur, de chez eux. Les entreprises ont dû s'adapter et commencer à offrir une expérience utilisateur conviviale sur leurs sites web. Aujourd'hui, les gens commandent leurs courses sur leur smartphone et les font livrer chez eux alors qu'ils sont au travail, ou regardent leurs films et séries préférés n'importe quand, où qu'ils se trouvent et sur des terminaux de tous types. Des sociétés comme Amazon et Netflix placent la barre de plus en plus haut en termes de fluidité des expériences clients sur tous les canaux, et les consommateurs attendent la même chose de toutes les marques avec lesquelles ils sont en contact. Y compris la vôtre... En bref, les entreprises n'ont plus le choix, il leur faut répondre à cette demande et offrir une expérience d'accès moderne et performante.



AVERTISSEMENT

D'après PwC (The Future of Customer Experience, 2018), 32 % des consommateurs se détourneront d'une marque jusque-là appréciée après une seule expérience négative, et cette proportion monte à 59 % après deux mauvaises expériences. Sachant cela, vous croyez réellement que vos clients attendront sagement la fin d'un processus de connexion qui prend plusieurs minutes ?

Une solution d'identité client de pointe qui contribue au déploiement d'une expérience optimale est indispensable, car elle permet aux entreprises de relever les défis suivants :

- » **Unifier les expériences numériques sur tous les terminaux** – Les clients n'apprécient pas de devoir s'enregistrer ou se connecter plusieurs fois pour accéder aux différents services d'une seule entreprise. Ils recherchent une expérience uniforme et entièrement fonctionnelle en toutes circonstances : qu'ils visitent votre site web sur leur ordinateur ou leur mobile, ou qu'ils utilisent les différentes applications mobiles de votre environnement numérique. Cette expérience doit donc inclure la possibilité de se connecter de façon fluide et sécurisée, partout dans le monde et à tout moment, sur des interfaces où la marque est immédiatement reconnaissable.
- » **Personnaliser le parcours client** – En collectant des informations faisant autorité sur les préférences (y compris en matière de consentement) directement auprès des utilisateurs et sur vos différents canaux, vous obtiendrez une visibilité complète sur vos clients. De là, vous pourrez consolider les identités et profils de vos clients en les stockant dans un emplacement unique, et personnaliser leur parcours en fonction de leurs préférences individuelles. Plus vos clients ont l'impression que vous comprenez leurs besoins, plus ils seront susceptibles d'acheter vos produits et services, puis de formuler des évaluations positives.
- » **Offrir des expériences inédites et sophistiquées** – La technologie évolue à un rythme effréné et contribue à modeler les attentes des clients et les tendances de consommation. Il y a dix ans, les smartphones servaient essentiellement à passer des appels et à consulter les e-mails personnels. Aujourd'hui, les consommateurs peuvent commander un article sur leur smartphone alors qu'ils sont dans les transports en commun, et demander sa livraison dès le lendemain. Avec une solution d'identité client performante, vous pouvez proposer une expérience fluide, avec des innovations telles que l'authentification sans mot de passe (par reconnaissance faciale ou empreinte digitale, par exemple), et ce, quel que soit le terminal.



Les solutions de gestion des identités clients et des identités collaborateurs sont des outils désormais incontournables dans la pile technologique d'une entreprise. Cependant, s'il y a peu de

risques que vos collaborateurs quittent l'entreprise à cause d'une expérience de connexion médiocre, vos clients, eux, ne vont pas y réfléchir à deux fois : ils iront voir ailleurs si vous ne parvenez pas à leur offrir une expérience optimale de bout en bout, notamment avec un processus de connexion fluide, personnalisé et omnicanal.

Renforcer la confiance

La réussite d'une entreprise repose en bonne partie sur sa capacité à gagner la confiance des consommateurs. Cependant, les données à caractère personnel et informations de compte qu'elle collecte et gère dans le cadre de ses activités sont constamment sous la menace d'une cyberattaque. Les cas de compromissions sont encore trop nombreux, et protéger les comptes et informations de vos clients est un impératif absolu. S'ils ne vous font pas confiance, ils passeront vite à la concurrence.



Quand des clients vivent une mauvaise expérience avec une entreprise ou perdent confiance en elle, il y a de fortes chances qu'ils partagent leur frustration avec le monde entier. Bienvenue dans le monde merveilleux des réseaux sociaux !

Les cybermenaces n'ont jamais été aussi sophistiquées, dévastatrices et fréquentes qu'aujourd'hui, avec une force de frappe jamais vue. La pandémie mondiale n'a apporté aucune trêve : les compromissions ont touché près de 16 milliards d'enregistrements au premier semestre 2020, soit une hausse de 273 % par rapport au premier semestre 2019, selon le site Security Boulevard (<https://securityboulevard.com>).

Du point de vue des clients, une brèche de données est indéniablement dévastatrice, tant sur le plan financier que personnel. Un particulier peut mettre des années à se remettre d'une usurpation d'identité et/ou d'un transfert d'argent frauduleux à la suite d'une cyberattaque. Certaines victimes sont affectées à jamais.

Pour les entreprises, les dommages financiers peuvent facilement dépasser les dizaines ou centaines de millions d'euros. En 2018, des cybercriminels ont dérobé les données de plus de 380 millions de clients de la chaîne hôtelière Marriott International. Après

divulgaration, cette brèche a coûté à Marriott plus de 44 millions de dollars dans les trois premiers mois qui ont suivi, auxquels il a fallu ajouter 25 millions de dollars d'amende de l'autorité britannique chargée de la protection des données (Information Commissioner's Office). Mais il est impossible de quantifier la perte de revenus résultant d'une image de marque entachée et de la fuite des clients. De nombreuses entreprises n'y survivent pas.

C'est pourquoi il est fondamental de mettre en place une solution d'identité client avancée, qui propose différentes manières de gagner et de conserver la confiance des clients :

- » **Sécuriser les comptes clients** – Comme nous l'avons évoqué, les cyberattaques sont de plus en plus sophistiquées et destructrices. Les mots de passe ne suffisent pas à protéger les comptes, en plus d'être pénibles à gérer. Avec l'authentification multifacteur (MFA) et l'authentification sans mot de passe, par exemple, vous pouvez sécuriser la totalité du cycle de vie de l'identité des clients, en les protégeant dès leur enregistrement sur vos applications, lors de leur authentification et pendant l'utilisation.
- » **Gérer la confidentialité et le consentement** – Pour leurs informations personnelles, les clients exigent sécurité et confidentialité. Le droit fondamental à la confidentialité des données est désormais inscrit dans de nombreuses lois, parmi lesquelles le règlement général sur la protection des données (RGPD) de l'Union européenne et le California Consumer Privacy Act (CCPA) aux États-Unis. Votre solution d'identité client doit vous permettre d'offrir une expérience client fluide et intuitive, par laquelle les consommateurs pourront gérer les informations personnelles qu'ils vous autorisent à utiliser, partager et enregistrer. Si votre plateforme de gestion des identités ne peut pas prendre en charge les dernières réglementations, vous faites courir un risque juridique sérieux à votre entreprise.
- » **Respecter les exigences réglementaires** – Le RGPD et le CCPA ne sont que deux exemples de réglementations strictes en matière de sécurité et de confidentialité, mais il en existe des dizaines que les gouvernements du monde entier ont adoptées ces dernières années. Et cette tendance n'est pas près de s'arrêter à plus ou moins brève échéance. Par exemple, le CCPA n'était même pas entré en vigueur depuis un an que le California Privacy Rights Act (CPRA)

a été promulgué en novembre 2020. Les entreprises qui ne parviennent pas à se conformer aux réglementations applicables risquent de perdre de l'argent, car elles échoueront aux audits et/ou seront obligées de cesser leurs activités.

Accélérer la transformation digitale

Aujourd'hui, les entreprises doivent adopter la technologie pour survivre et prospérer. La transformation digitale concerne chaque secteur d'activité, et cette tendance s'accélère d'année en année. Par exemple, les vidéoclubs, et même certains cinémas, ont disparu sous l'effet des services de streaming, et les sociétés de taxi luttent pour rivaliser avec les voitures de transport avec chauffeur, ou services VTC. Cependant, dans la migration de leurs systèmes hérités peu performants, de nombreuses entreprises risquent d'enregistrer un déficit technique considérable. La transformation digitale exige une modernisation de l'infrastructure technologique, et sans doute une transition vers l'économie des API (Application Programming Interface).



TECHNIQUE

Le déficit technique est le coût implicite du retravail causé par une décision d'implémenter une solution plus simple, mais pas forcément appropriée.

Les entreprises ont besoin d'une solution d'identité client avancée qui les aide à mener et accélérer leur transformation digitale, en particulier:

- » **Migrer vers le cloud** – Le cloud fait partie intégrante de la stratégie de transformation digitale de la plupart des entreprises. Une infrastructure d'ancienne génération entrave la flexibilité de l'entreprise et sa capacité à offrir l'expérience que les clients attendent. Cependant, une migration vers le cloud peut prendre des années. Pour résoudre ce problème, il est possible de mettre en place une seule couche d'identités non seulement pour les applications web et mobiles, mais aussi pour les applications on-premise héritées. Il est alors plus facile de gérer ces environnements cloud hybrides composés de ressources de cloud public, cloud privé et on-premise. Parmi les avantages du cloud :
 - *Plus grande agilité dans le développement et le déploiement d'applications, allée à une réduction des*



coûts: les entreprises peuvent déployer rapidement des services et ressources cloud, et les faire évoluer à la demande. Ainsi, elles peuvent déclasser une infrastructure d'identités héritée et éliminer les coûts liés à une maintenance continue.

- *Utilisation d'une architecture de microservices et d'API*: de nos jours, les développeurs créent des applications qui exploitent des microservices et des API. Ce type d'architecture nécessite une approche globale et centralisée de la gestion des identités afin d'offrir un accès sécurisé à vos clients et partenaires. Avec une solution d'identité client native au cloud, vos développeurs peuvent facilement intégrer des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs dans les applications qu'ils créent, et donc se concentrer davantage sur les activités stratégiques.

Les *microservices* sont de petits services conteneurisés, déployables de façon indépendante et partiellement connectés, qui constituent les composants d'une application. Une API (Application Programming Interface) permet à différentes applications de communiquer entre elles via une connexion logicielle.

- » **Entrer dans l'économie des API** – Les API représentent désormais bien plus qu'une simple technique de développement. Elles sont devenues un véritable moteur du modèle de vente, et permettent à l'entreprise de diversifier ses sources de revenus en monétisant l'accès à ses API propriétaires. À titre d'exemple, une API peut permettre d'intégrer une carte géographique à une application VTC, ou de sécuriser les paiements sur une application de livraison de repas via un compte de réseau social. Grâce à une solution d'identité client de pointe capable de contrôler les API et d'en sécuriser l'accès, l'entreprise peut étendre ses activités basées sur les API en toute sécurité.

- » **Création d'expériences clients fluides et sécurisées**
- » **Utilisation judicieuse des ressources limitées de votre équipe de développement**
- » **Intégration à la pile technologique pour plus de fiabilité et des délais de lancement accélérés**
- » **Calcul du coût total du développement en interne par comparaison à l'achat d'une solution**

Chapitre 3

Mise en place de la gestion des identités clients

Le chapitre 2 a détaillé les raisons pour lesquelles une solution d'identité client avancée est une nécessité : offrir une expérience client optimale, susciter la confiance des consommateurs et accélérer la transformation digitale. À ce stade, peut-être pensez-vous : « Pas de problème, je peux le faire moi-même ». Mais ce n'est malheureusement pas aussi simple, et nous tenons à vous mettre en garde avant que vous ne vous lanciez dans des projets de développement risqués. Nous vous expliquons pourquoi dans ce chapitre.

Expérience client vs sécurité et conformité, un équilibre difficile

Développer une solution d'identité client exige de trouver un équilibre entre deux exigences clés qui sont parfois diamétralement opposées : offrir une expérience client optimale tout en assurant la sécurité et la conformité.

Prenez deux minutes pour réfléchir à ce qui, pour vous, constitue une expérience idéale. Après tout, c'est vous le client dans bon nombre de vos interactions personnelles au quotidien. Qu'est-ce qui vous apporte de la satisfaction dans votre navigation en ligne ? Par exemple, votre expérience idéale en tant que client peut inclure :

- » **Un processus d'enregistrement qui se déroule sans encombre** – La première fois que vous visitez un site web ou utilisez une application, le processus d'onboarding doit être simple et rapide. Par exemple, certains sites demandent juste quelques informations bien ciblées lors de votre visite initiale et par la suite ; vous n'êtes pas obligé de raconter votre vie dès le départ. Cette pratique est connue sous le nom de *progressive profiling*.
- » **Un processus de connexion intuitif et fluide** – Le processus de connexion doit prévoir plusieurs méthodes d'authentification personnalisées selon vos préférences personnelles. En général, les clients préfèrent éviter les mots de passe, et ils apprécient de ne pas être obligés d'en créer et mémoriser de nouveaux – grâce à une authentification utilisant un compte de réseau social, par exemple, ou la reconnaissance faciale sur un smartphone.
- » **Une authentification unique sur les différentes applications d'une même entreprise** – Un portail clients doit intégrer de façon fluide toutes vos applications dans une seule expérience de connexion.
- » **Une expérience client associée à une marque** – Le client doit pouvoir reconnaître immédiatement les marques qu'il aime et auxquelles il fait confiance, même dans le cas d'applications ou de services différents fournis par la même entreprise (comme Amazon Prime Video et Whole Foods, accessibles sur le même site Amazon).

- » **Une expérience omnicanale dans n'importe quelle langue** – Bénéficiez d'une expérience de connexion uniforme sur n'importe quel terminal, à tout moment et partout dans le monde, dans votre langue d'expression.
- » **Des recommandations personnalisées** – Obtenez des recommandations de produits et services pertinentes en fonction de votre profil et de votre historique d'achats.

Autrement dit, pour offrir une expérience de premier plan avec votre solution d'identité client, vous devez d'abord définir les attentes de vos clients. Et non seulement ces attentes sont nombreuses, mais elles peuvent différer fortement d'une personne à l'autre : ce qui enchante un consommateur en rebutera un autre.

L'IDENTITÉ CLIENT, UNE NÉCESSITÉ AUSSI POUR LE B2B

Bien que ce chapitre concerne principalement le modèle B2C (business-to-consumer), les applications destinées au B2B (business-to-business) doivent aussi offrir une expérience client fluide et intuitive. Dans de nombreuses relations B2B, une entreprise vend et l'autre achète. De nombreuses exigences liées à l'identité client sont donc similaires entre le B2B et le B2C. Vous pouvez également ajouter un certain nombre de critères supplémentaires propres au B2B, par exemple la capacité à se connecter au site web ou à l'application d'un partenaire via vos identifiants d'entreprise, plutôt que de créer un nouveau compte.

Répondre aux impératifs de sécurité et de conformité tout en offrant une expérience client fluide est en soi un immense défi.

Si vous envisagez sérieusement de développer votre propre solution de gestion des identités clients, vous devez être conscient d'un certain nombre de difficultés :

- » **Vous partez de zéro et devez tout créer. Bon courage.** Vous devez créer des méthodes de sécurité que vos

clients acceptent et dont ils ont besoin. Il peut s'agir de l'authentification multifacteur (MFA), de l'authentification multifacteur adaptative (AMFA) demandant des facteurs d'authentification supplémentaires uniquement en cas de risque élevé, de l'authentification sans mot de passe, de la connexion par mot de passe à usage unique (OTP), etc.

- » **Garder une longueur d'avance sur les cybercriminels est un combat sans fin.** Même les équipes sécurité dédiées sont engagées dans une lutte constante pour ne pas se laisser déborder par les nouvelles vulnérabilités. De plus en plus, les cybermenaces et attaques sophistiquées tirent parti d'identifiants de comptes en ligne compromis. Si vous développez votre propre solution d'identité client, vous ne manquerez pas d'attirer les cybercriminels. Vous allez devoir faire en sorte que votre solution maison ne remplace pas les utilisateurs en qualité de maillon faible de votre sécurité.
- » **Les demandes des clients évoluent en permanence.** Aujourd'hui, ils veulent en finir avec les mots de passe. Demain, ils décideront peut-être que les codes envoyés par SMS sont trop compliqués. Bref, les satisfaire à long terme est un vrai défi. Si l'identité client n'est pas votre cœur de métier, votre solution développée en interne va venir allonger la liste des éléments que vous devez constamment ajuster pour préserver la satisfaction de vos clients.
- » **Le paysage de la conformité est en profonde mutation.** Il change constamment et se complexifie d'année en année. Le règlement général sur la protection des données (RGPD) de l'Union européenne, et les lois HIPAA (Health Insurance Portability and Accountability Act) ou CCPA (California Consumer Privacy Act) aux États-Unis ne sont que quelques-unes des réglementations de sécurité et de confidentialité qui n'ont cessé d'être promulguées, actualisées, remplacées et révisées ces dernières années. Avec un tel enchevêtrement d'exigences souvent conflictuelles, difficile d'y voir clair. Comprenez bien que, si votre solution maison ne respecte pas ces différentes réglementations, votre entreprise risque gros en termes d'amendes et autres sanctions.

Enfin, toujours dans le cas où vous persistez à vouloir développer votre propre solution d'identité client, vous devrez faire face à d'autres contraintes :

- » **L'innovation en matière de sécurité ne s'arrête jamais,**

et vous devrez tenir le rythme. Si vous voulez que votre entreprise reste toujours à la pointe de la technologie, les fonctionnalités innovantes que vous prévoyez de développer (AMFA, authentification sans mot de passe, identification biométrique, mots de passe à usage unique, etc.) devront être évolutives. Cependant, elles devront aussi permettre une utilisation aussi fluide que possible pour vos clients. C'est la première contrainte, car mettre en place un facteur d'authentification supplémentaire équivaut à introduire un nouveau point de friction.

» **Les collaborateurs internes d'une entreprise ont une vision et des priorités différentes.** Le marketing réclame une expérience utilisateur fluide et optimale. Le service commercial fait les gros yeux, car il voulait lancer le produit au plus vite. L'équipe sécurité exige un accès ultrasécurisé avant tout. Les développeurs et ingénieurs préfèrent se concentrer sur leur produit plutôt que sur des fonctions d'authentification. Le service financier attend un ROI maximal avec un investissement minimal. Et votre PDG veut tout.



RAPPEL

D'un côté, pour offrir une expérience client de premier plan, les entreprises doivent permettre un accès rapide et facile à leurs applications, au moyen d'un processus fluide et intuitif d'enregistrement et de connexion. De l'autre, les clients attendent des entreprises qu'elles protègent leurs informations personnelles et leur confidentialité. Si vos clients n'ont pas confiance en vous, ils iront voir ailleurs. Avant de vous lancer dans le développement de votre propre solution d'identité client, réfléchissez aux difficultés qu'implique l'atteinte du juste équilibre entre, d'une part, une expérience client fluide et, d'autre part, une sécurité et une conformité inattaquables. Abordez ensuite la question avec vos développeurs (voir la section suivante).

Attirer et retenir des développeurs compétents

Vous disposez de développeurs expérimentés ? De classe mondiale, dites-vous ? (Et c'est pour cela que vous les payez si cher.) Soit. Mais la vraie question est : votre équipe est-elle assez fournie

? Face à la pénurie mondiale de développeurs compétents, les entreprises se livrent à une bataille rangée pour attirer et retenir les talents.

Il existe toutefois une autre catégorie de professionnels IT qui sont devenus plus rares que l'ours polaire : les ingénieurs sécurité. Si vous comptez dans votre équipe un développeur capable de créer des fonctionnalités d'identité client sécurisées assurant une expérience client optimale, une sécurité et confidentialité hors pair et une conformité réglementaire continue, vous pouvez vous targuer d'avoir déniché la perle rare. Cependant, à moins que votre cœur de métier ne soit la gestion des identités et des accès (IAM), il ne rime pas à grand-chose d'affecter cette perle rare au développement d'une solution d'identité client. Vos développeurs sont précieux, alors ne devraient-ils pas plutôt être mobilisés à 100 % sur vos activités stratégiques ainsi que sur les applications et sites web générateurs de revenus ?



Le développement d'une solution d'identité client implique d'écrire énormément de code personnalisé. Or, selon le Top 10 de l'OWASP (Open Web Application Security Project <https://owasp.org>), 93 % des vulnérabilités d'applications sont découvertes dans du code personnalisé. Ces vulnérabilités exposent votre entreprise et vos clients à des failles de sécurité majeures et génèrent un déficit technique considérable ainsi que des coûts d'opportunité. Mais ce n'est pas tout. D'après le site Stripe.com (<https://stripe.com/files/reports/the-developer-coefficient.pdf>), les développeurs passent 42 % de leur temps sur le débogage et la maintenance de code hérité de mauvaise qualité, ce qui est du temps en moins consacré au développement de nouvelles applications. Si vous n'avez rien de mieux à proposer à vos développeurs que de faire la chasse aux bugs, vous risquez d'avoir encore plus de mal à les attirer et à les retenir.

Autres considérations

À ce stade, vous avez déjà deux impératifs : offrir une expérience client fluide tout en assurant la sécurité et la conformité, et faire en sorte que vos développeurs (ressource précieuse) restent concentrés sur vos activités stratégiques. À cela s'ajoutent d'autres défis dont vous devrez tenir compte si vous décidez de

développer votre propre solution d'identité client :

- » **Nécessité d'une évolutivité à grande échelle** – Les clients veulent pouvoir accéder de façon sécurisée et fluide à vos applications mobiles, sites de vente et portails partenaires, sur n'importe quel terminal, en tout lieu et à tout moment de l'année — pendant les soldes, lors des fêtes de fin d'année, à l'annonce des concerts et événements sportifs majeurs, à la sortie du dernier blockbuster et, plus généralement, pendant toutes les périodes de forte demande. Toute indisponibilité vous fera perdre des revenus et nuira à votre image de marque. Le processus de conception, développement et maintenance de l'infrastructure requise pour assurer un service fiable à grande échelle est complexe et coûteux. Êtes-vous réellement sûr de vouloir gérer votre propre infrastructure, et avec elle les pannes, les temps d'arrêt pour maintenance et les mises à niveau ?
- » **Intégration avec votre pile technologique** – Pour que vous puissiez étendre les fonctionnalités et maximiser le ROI de votre solution d'identité client, celle-ci doit pouvoir se connecter en toute sécurité aux autres outils et applications de votre environnement technologique, notamment à tous les logiciels liés à la sécurité, à la confidentialité, au marketing et aux services.
- » **Accélération des délais de lancement** – Afin de répondre à des attentes de plus en plus élevées, et de limiter l'exposition à des risques de sécurité et de conformité de plus en plus complexes, les entreprises doivent proposer des expériences clients fluides, sécurisées et innovantes le plus vite possible. Comme vous l'aurez maintenant compris, la création en interne de fonctionnalités d'identité client personnalisées répondant à ces critères est un parcours difficile et coûteux au fil du temps. Et qu'en sera-t-il si vos clients ne veulent plus utiliser les SMS pour s'authentifier, ou si vous devez répondre aux exigences réglementaires d'un nouveau pays dans lequel vous vous implantez ? Créer une solution d'identité client n'est pas un effort ponctuel, limité dans le temps. C'est un cycle perpétuel qui exige une innovation continue et un travail de développement produit permanent pour suivre l'évolution rapide des attentes du marché et des menaces de sécurité.

Une décision classique : acheter ou développer ?

Développer une solution d'identité client répondant aux besoins spécifiques de vos clients est extrêmement difficile. Il est également très coûteux d'en assurer la maintenance à long terme. Un tel projet nécessite de bien cerner le type d'expérience que vos clients attendent (à la fois fluide et sécurisée) ; de mettre en place une équipe de développeurs chevronnés (c'est-à-dire rares et coûteux) pour écrire et maintenir un code sécurisé ; d'établir une infrastructure complexe et onéreuse pour assurer un accès permanent à grande échelle ; et de créer des intégrations avec votre pile technologique tout en accélérant les délais de lancement des nouvelles fonctionnalités de vos applications stratégiques.

Avant de vous lancer dans une initiative de ce genre, prenez le temps de calculer son coût total, en incluant le déficit technique, les risques de brèches de sécurité et les coûts d'opportunité.



RAPPEL

Si la création en interne d'une solution d'identité client est difficile (et inutile), ne faites pas non plus de compromis lors de votre achat. Dans le chapitre 4, vous allez découvrir les atouts d'une solution d'identité client avancée pour entreprise, et le chapitre 5 vous expliquera les fonctionnalités que vous devez en attendre.

- » **En quoi consiste une solution d'identité client avancée**
- » **Les avantages du modèle plateforme**
- » **Une infrastructure de services sécurisée, fiable et évolutive**
- » **Étude de cas d'usage et témoignages clients**

Chapitre 4

Les atouts d'une solution d'identité client avancée

Comme nous l'avons expliqué dans le chapitre 3, il est extrêmement difficile et coûteux de développer soi-même une solution d'identité client. Détourner vos développeurs, une ressource précieuse et limitée, de projets liés au cœur de métier pour les faire travailler sur une solution d'identité client maison n'a pas beaucoup de sens. Dans ce chapitre, nous expliquons pourquoi la décision de collaborer avec un spécialiste en gestion des identités clients est certainement la plus judicieuse, car cet expert pourra vous aider à résoudre vos défis et à proposer une expérience fluide et sécurisée à vos clients.

Qu'est-ce qu'une solution d'identité client ?

Une solution d'identité client de pointe fournit une couche d'identité numérique qui peut s'intégrer rapidement et harmonieusement à vos applications, sites web et portails orientés clients. Ce type de solution aide les entreprises à répondre aux attentes de leurs clients et à gagner leur confiance en leur offrant une expérience fluide, en raccourcissant les délais de lancement, en gérant de façon centralisée les politiques d'identification et d'accès, et en renforçant la sécurité à l'échelle d'Internet.

Des expériences utilisateurs optimales

Pour proposer des expériences fluides, vous devez connaître et comprendre vos clients. Avec une solution d'identité client avancée, vous bénéficiez d'une vue à 360 degrés de vos clients dès qu'ils utilisent les applications et produits de votre marque, indépendamment du terminal et du lieu d'où ils se connectent. Vous pouvez ensuite utiliser ces informations pour proposer des expériences sur mesure tout en limitant les points de friction de différentes façons :

- » En offrant une expérience client uniforme et cohérente sur l'ensemble de vos applications et sites web, ce qui évite aux utilisateurs de devoir se connecter à chacun d'eux.
- » En demandant moins, voire plus du tout, de mots de passe sur tous vos canaux et sur tous les terminaux des clients.
- » En limitant la quantité d'informations demandées aux prospects lorsqu'ils s'enregistrent.
- » En permettant à vos partenaires commerciaux de se connecter avec leurs identifiants d'entreprise, ce qui leur évite de devoir créer de nouveaux noms d'utilisateur et mots de passe.
- » En employant des interfaces personnalisées qui reflètent votre marque, pour susciter la confiance des clients.



Le progressive profiling permet de collecter des informations utilisateurs tout au long du parcours client. C'est une bonne alternative aux processus d'enregistrement interminables. Avec l'authentification sociale, vos utilisateurs peuvent partager (à condition qu'ils soient d'accord) des informations de base issues de leurs comptes de réseaux sociaux. Comme ils n'ont plus besoin de saisir ces données manuellement, ils peuvent accéder plus vite à vos services.

Des délais de lancement accélérés

Une solution d'identité client de pointe inclut une panoplie d'outils permettant d'intégrer rapidement et efficacement des fonctionnalités de gestion des identités et des accès dans vos applications, sites web et portails orientés clients, vous permettant d'accélérer vos délais de lancement. Ces outils sont très divers : ils vont des solutions prêtes à l'emploi, faciles à configurer et rapides à déployer pour les entreprises ayant des besoins simples en matière d'identité et préférant les déploiements low-code, jusqu'à une longue série d'API et SDK pour les organisations avec des besoins plus complexes, nécessitant une personnalisation poussée. Grâce à ces outils, vos équipes de développement peuvent rapidement intégrer les fonctionnalités d'identité client dans les expériences clients, plutôt que de les créer de A à Z, ce qui réduit les délais de lancement.

Une gestion centralisée

Lorsque le nombre des expériences que vous proposez à vos clients augmente sur vos canaux, il devient indispensable de centraliser la gestion des identités et des accès. Une source fiable unique pour les identités de tous vos utilisateurs, groupes et terminaux peut alors évoluer avec votre entreprise. Vous bénéficiez d'une interface centralisée et uniforme avec laquelle vous pouvez gérer toutes les règles d'accès, les politiques de sécurité et l'appartenance aux groupes, ce qui réduit votre charge d'administration. En outre, vous renforcez la cohérence, limitez les erreurs de configuration, évitez les failles de sécurité et assurez la conformité.



Gérer les identités et les accès d'une application à la fois est inefficace et risqué. Cette méthode demande des efforts inutiles et vous rend vulnérable aux failles de sécurité, car elle ne permet pas de garantir l'exécution cohérente de vos politiques d'accès et de sécurité sur la totalité de votre environnement numérique.

Une sécurité à l'échelle d'Internet

Une solution d'identité client avancée est conçue sur une plateforme cloud sécurisée, gérée par le fournisseur de services. Comme les opérations de sécurisation et de mise à jour de la plateforme ou des composants d'infrastructure sous-jacents relèvent de la responsabilité du fournisseur de services, vous n'avez plus à vous en préoccuper.

En outre, ce type de solution comporte des fonctionnalités de sécurité sophistiquées, comme la MFA adaptative, qui font appel à un large éventail de facteurs et prennent en compte à la fois le contexte et le paysage des menaces. Des rapports d'analyse et tableaux de bord détaillés donnent une visibilité en temps réel sur les menaces et attaques potentielles, ce qui permet aux équipes d'identifier les problèmes, de les étudier et de les corriger rapidement.



RAPPEL

Une solution d'identité client avancée vous apporte les dernières innovations en matière de sécurité, comme les politiques basées sur les risques et l'authentification sans mot de passe, sans avoir besoin de les créer vous-même. Vos équipes de développement peuvent ainsi se consacrer pleinement à vos activités stratégiques au lieu d'essayer de contrer les dernières menaces de sécurité.

Le modèle plateforme

Les solutions d'identité client avancées adoptent un modèle plateforme pour la gestion des identités et des accès (IAM). Ainsi, elles peuvent prendre en charge n'importe quels cas d'usage, utilisateurs et technologies.

Ce type de conception vous permet de trouver des synergies IAM entre vos divers types d'utilisateurs, dont vos collaborateurs, partenaires et clients, indépendamment de leur emplacement géographique, de leurs applications et de leurs terminaux. Par exemple, un partenaire B2B (business-to-business) qui revend vos produits et un responsable de comptes interne devront très probablement accéder aux mêmes types de ressources : applications et outils commerciaux, catalogues de produits, etc. Une solution d'identité client développée en interne sera certainement créée par différentes équipes produits : une consacrée aux cas d'usage

internes, l'autre aux partenaires externes. Chaque équipe mettra au point une expérience utilisateur différente et établira chacune ses propres politiques de sécurité et d'accès, gaspillant ainsi un temps et des ressources précieux. L'expérience utilisateur qui en résultera sera en outre incohérente, avec potentiellement l'introduction de nouveaux risques de sécurité. À l'inverse, une solution basée sur une plateforme unique assure une approche IAM cohérente pour tous les utilisateurs finaux et optimise les synergies.



CONSEIL

Par ailleurs, le modèle de plateforme indépendante et neutre permet également d'étendre les capacités de gestion des identités clients en intégrant vos ressources numériques à n'importe quelle technologie. Vous pouvez connecter vos applications on-premise et cloud en toute transparence pour offrir à vos clients un accès unifié à vos produits hérités et modernes, tout en exploitant les points de données de vos outils préférés grâce à des préintégrations à des technologies de pointe. Par exemple, vous pouvez envoyer les coordonnées des utilisateurs collectées pendant le processus d'enregistrement à un outil marketing qui automatise l'envoi d'informations aux clients.

Une infrastructure de développement sécurisée, fiable et évolutive

Les entreprises qui tentent de créer leur propre solution d'identité client doivent relever un défi permanent et coûteux : concevoir, développer et maintenir une infrastructure qui offre la sécurité, la fiabilité et l'évolutivité requises.

Une infrastructure mal sécurisée fait fuir les clients, car ils n'ont pas confiance en votre marque. Si elle n'est pas fiable, les utilisateurs ne pourront même pas accéder à vos services, car votre site sera souvent en panne. Si elle n'est pas évolutive, de nombreux clients se lasseront d'attendre qu'une connexion s'établisse pendant les pics de trafic et iront voir ailleurs.



RAPPEL

Une solution d'identité client avancée est construite sur une infrastructure cloud-native sécurisée, fiable et évolutive, proposée en tant que service.

Ainsi, vous n'avez plus besoin de recruter en interne des experts en infrastructure, de budgétiser vos coûts d'utilisation de l'infrastructure cloud ou de faire monter en charge vos systèmes pour répondre aux pics de la demande. Vous ne devez plus non vous occuper des correctifs et mises à niveau système et logiciels, qui nécessitent des fenêtres de maintenance au cours desquelles vos services sont interrompus.

Pour assurer la fiabilité, une solution d'identité client de pointe doit offrir une redondance extrême à chaque couche de la pile d'infrastructure au cas où une connexion serveur ou réseau (par exemple) s'interrompt. Cette infrastructure redondante doit inclure des workflows automatisés capables de rediriger le trafic sur plusieurs zones géographiques, condition indispensable pour offrir une disponibilité maximale sans nécessiter d'intervention humaine.

L'évolutivité nécessite des capacités à la demande qui peuvent augmenter ou diminuer automatiquement, selon les besoins. Ainsi, vous ne gaspillez plus d'argent sur des ressources inutilisées et vous ne perdez plus de revenus en raison d'une capacité insuffisante.

ARDUINO

Arduino contribue à démocratiser la révolution de l'Internet des objets (IoT) en rendant les logiciels et le matériel open source accessibles aux enseignants, étudiants et créateurs en tout genre. Comme Arduino est une société basée en Europe, elle se trouve sous la juridiction du RGPD et prend donc très au sérieux la confidentialité et la sécurité.

La plateforme Auth0 by Okta s'est avérée cruciale pour aider Arduino à maintenir sa conformité et à assurer de hauts niveaux de sécurité, en lui permettant de déployer rapidement l'authentification à deux facteurs. Arduino a aussi pu accélérer sa mise à l'échelle en permettant à ses développeurs de lancer ses produits plus vite.

Pour son application Arduino IoT Cloud, les développeurs avaient besoin de se connecter à la fois à l'IoT et à Android. Ils ont pu implémenter chacune de ces connexions en deux jours et demi, et ainsi déployer rapidement ce produit en quelques semaines.

SIEMENS

Avec sa grande diversité de divisions et d'opérations, Siemens avait désespérément besoin de standardiser et de sécuriser ses processus de connexion. Il y a deux ans, l'entreprise a choisi Auth0 pour l'aider à créer une expérience de connexion uniforme pour ses clients et ses partenaires.

De cette coopération est né Siemens ID, un service de connexion unique qui peut être intégré rapidement à la pile applicative de chaque division de l'entreprise. Aussi bien les clients que les partenaires utilisent désormais Siemens ID pour accéder aux centaines d'applications et services Siemens dans le monde. Siemens ID centralise le stockage de la base de données utilisateurs et de la page de connexion, tout en permettant à chaque division d'intégrer l'application à sa manière unique.

Pour assurer la sécurité, vous devez rester au courant des dernières menaces et vulnérabilités qui peuvent affecter toute la pile technologique de votre infrastructure.



CONSEIL

Un fournisseur externe spécialisé en identité client peut gérer toutes ces exigences pour vous, ce qui vous laisse libre de vous consacrer pleinement à votre cœur de métier.

Étude de cas d'usage

Une solution d'identité client de premier plan permet de prendre en charge un riche éventail de cas d'usage et donc de répondre à des besoins métier très variés. Dans les sections suivantes, nous allons explorer quelques cas d'usage courants ainsi que des témoignages de clients Okta.

BAZAARVOICE

Après plusieurs années de croissance rapide, Bazaarvoice avait du mal à gérer l'identité dans ses multiples applications clients cloisonnées. L'équipe IT a été chargée de centraliser les identités utilisateurs au sein de la suite de produits de la marque.

Bazaarvoice effectue l'onboarding des utilisateurs dans les nouvelles applications connectées, mais étudie actuellement les fonctionnalités Inbound Federation d'Okta, qui pourraient permettre aux clients de se connecter via leur propre fournisseur d'identité. La fédération simplifierait la gestion des utilisateurs et permettrait à la marque de se dégager de ses responsabilités en termes d'authentification et de stockage de données — un avantage non négligeable au vu des quelque 590 millions de consommateurs qui interagissent chaque mois avec ses applications.

XERO

Alors que Xero se préparait à une forte croissance très tôt dans son développement, son équipe IT recherchait un partenaire de gestion des identités capable de l'aider à sécuriser son infrastructure applicative et d'automatiser ses processus. Okta Workflows s'est avéré la solution parfaite.

Créer un processus automatisé en rédigeant du code personnalisé implique fréquemment d'utiliser une clé, un jeton ou un mot de passe pour appeler une API tierce. Ce jeton est souvent stocké dans un fichier sur le serveur de l'entreprise, où il n'est pas forcément très bien protégé. Comme Okta Workflows s'exécute sur la plateforme Okta plutôt que sur un ordinateur ou serveur on-premise, les jetons API sont automatiquement sécurisés et mis à jour.

Protection contre le piratage de comptes

Le piratage de comptes est une méthode d'attaque d'usurpation d'identité de plus en plus courante, par laquelle un cybercriminel accède de façon non autorisée au compte d'un utilisateur pour lui dérober de l'argent ou des données. Ces attaques peuvent être lancées manuellement ou automatisées à l'aide de bots. Pour contrer cette menace, vous devez mettre en place une plateforme d'identité qui associe sécurité et expérience utilisateur fluide.

Des applications hautement évolutives

Les entreprises développent des applications et sites web pour attirer autant de clients que possible. Ainsi, votre solution d'identité client doit être fiable et évolutive, surtout lors des pics de trafic ou de demande – par exemple lors de la vente de billets pour un concert ou un événement sportif, ou d'une vente flash pendant les fêtes.

Des identités clients unifiées sur toutes les applications

Pour vos clients, créer de nouveaux comptes et gérer une flopée d'identifiants sur différents sites web et applications, surtout s'ils appartiennent à la même marque ou entreprise, n'est pas franchement une partie de plaisir. Si vous souhaitez leur offrir une expérience fluide, vous devez absolument unifier les identités de vos clients sur toutes vos propriétés numériques.

Intégration des identités d'entreprise

Avec une solution d'identité client avancée, les clients B2B n'ont plus besoin de créer des identités et identifiants séparés lorsqu'ils se connectent aux applications, sites web et portails de leurs partenaires. En effet, ce type de solution intègre les identités et identifiants d'entreprise, de sorte que les clients B2B peuvent les réutiliser sur les propriétés numériques de leurs partenaires.

Sécurisation de l'accès aux API

Pour les entreprises qui rejoignent l'économie des API (un point abordé au chapitre 2), protéger l'accès aux API est fondamental pour empêcher les cybercriminels d'exploiter les vulnérabilités ou d'acquérir un accès non autorisé aux applications connectées.

- » Principales fonctionnalités des solutions d'identité client
- » Prise en charge de tous les cas d'usage à l'aide d'une plateforme neutre et indépendante
- » Services fiables et sécurisés à grande échelle
- » Collaboration avec un leader du marché

Chapitre 5

Fonctionnalités incontournables d'une solution d'identité client avancée

Maintenant que vous savez comment l'identité client peut aider votre entreprise à offrir une expérience client fluide et sécurisée (voir le chapitre 4), vous pouvez commencer à évaluer les possibilités qui s'offrent à vous. Dans ce chapitre, vous découvrirez les fonctionnalités d'une solution d'identité client et les critères qui doivent guider votre choix.

Choisir le meilleur produit

Une solution d'identité client avancée doit offrir des fonctionnalités prêtes à l'emploi, faciles à configurer et rapides à déployer, ainsi que des outils conçus pour les développeurs, par exemple des API, des SDK et des hooks, qui permettront de personnaliser et d'étendre les fonctionnalités.

Voici les principales fonctionnalités prêtes à l'emploi dont vous devez disposer :

» **Authentification, autorisation et gestion des utilisateurs**

– le strict minimum de toute solution d'identité client qui se respecte (voir le chapitre 1). En plus de ces fonctionnalités de base, comptez également sur les fonctionnalités avancées suivantes :

- *Authentification* – Prise en charge de la connexion via les réseaux sociaux et du standard OpenID Connect (OIDC) générique, authentification SSO auprès des applications tierces, authentification sans mot de passe, authentification basée sur les risques, widget de connexion préintégré et branding personnalisé au niveau des applications.
- *Autorisation* – Gestion de l'accès aux API fondée sur OAuth 2.0 (Open Authorization), intégration avec les API gateways et contrôle des accès aux applications basé sur les rôles.
- *Gestion des utilisateurs* – Répertoire d'utilisateurs cloud hautement évolutif permettant de gérer tous vos utilisateurs, groupes et terminaux ; mappage des profils utilisateurs ; prise en charge de la méthode de migration des utilisateurs de votre choix (importation en masse, Just-In-Time, annuaire existant).

» **Flux utilisateurs redéfinis et personnalisables** capables d'offrir rapidement des fonctionnalités de support de premier plan aux utilisateurs et aux clients, comme l'enregistrement, la réinitialisation des mots de passe et la récupération des comptes/noms d'utilisateur en libre-service.

» **Interface d'administration intuitive et centralisée** et tableaux de bord de gestion personnalisables, qui donnent aux équipes sécurité et administration la possibilité de gérer les politiques de sécurité de façon cohérente et depuis un seul emplacement.

» **Authentification multifacteur (MFA) et authentification multifacteur adaptative (AMFA)** prenant en charge différents facteurs et méthodes — des plus basiques comme l'envoi d'e-mails et de SMS de validation, aux plus avancés comme la biométrie (par exemple, TouchID et FaceID). L'AMFA ajoute une couche intelligente d'authentification basée sur les risques qui exploite des informations contextuelles, par exemple sur la zone géographique et le

terminal de connexion, pour appliquer l'authentification multifactor (MFA) seulement lorsque c'est nécessaire.

- » **Provisioning automatisé en parallèle de la gestion du cycle de vie des utilisateurs**, avec notamment des workflows automatisés associés à l'étape du cycle de vie où vos clients se trouvent. Vous pouvez ainsi provisionner et déprovisionner les utilisateurs pour qu'ils accèdent aux applications et systèmes en aval sur l'intégralité de votre pile technologique. (Par exemple, l'accès au CRM est automatiquement octroyé à vos partenaires B2B dès le début du partenariat.)
- » **Intégration B2B (business-to-business)** pour connecter les applications et portails des partenaires, et fédérer les identités sur les annuaires d'entreprise, comme Active Directory et LDAP (Lightweight Directory Access Protocol). Les utilisateurs professionnels peuvent ainsi se connecter plus facilement, sans avoir à créer de nouveaux identifiants, et les entreprises disposent de données à jour sur ces utilisateurs.
- » **Intégration avec les applications on-premise héritées** pour offrir à vos clients un accès unifié à tous vos produits et accélérer votre transformation digitale.

Les entreprises qui ne souhaitent pas se contenter des fonctionnalités prêtes à l'emploi doivent opter pour une solution incluant une grande variété d'API, SDK et hooks qui prennent en charge les langages de programmation que votre équipe de développement utilise. Ces outils destinés aux développeurs vous aideront dans les opérations suivantes :

- » **Intégration rapide et efficace des fonctionnalités d'identité client dans vos applications** sans devoir les créer de A à Z.
- » **Personnalisation et adaptation de l'identité client selon vos besoins précis**, afin de pouvoir obtenir un avantage concurrentiel avec des expériences clients sur mesure.
- » **Utilisation de solutions de pointe présentes dans votre pile technologique** pour étendre vos fonctionnalités d'identité client et satisfaire vos clients (voir la section suivante pour plus de détails).

Choisir la bonne plateforme

Adoptez une solution d'identité client fondée sur une plateforme ouverte, indépendante et neutre, qui vous permettra de répondre en toute sécurité à n'importe quel cas d'usage relatif à l'identité, quels que soient les types d'utilisateurs finaux interagissant avec votre entreprise, tout en exploitant la technologie que vous voulez.

Choisissez une solution prenant en charge un large éventail d'utilisateurs finaux, ce qui inclut les clients, les partenaires et même vos collaborateurs. Un modèle plateforme constituera une fondation solide qui évoluera en même temps que vos besoins. Par exemple, imaginons que votre entreprise recherche une solution d'identité client incluant une intégration B2B prête à l'emploi pour se connecter au portail d'un partenaire. Un an plus tard, votre entreprise étend son activité au grand public et a besoin d'une fonctionnalité d'authentification sans mot de passe personnalisable pour sa nouvelle application B2C (business-to-consumer) mobile. Cela ne signifie pas que vous aurez besoin de deux solutions d'identité client distinctes. Une seule solution basée sur une plateforme unique est capable de prendre en charge les deux cas d'usage, ce qui diminue les coûts et renforce l'efficacité opérationnelle grâce à une administration et des workflows simplifiés. Par ailleurs, imaginons aussi que votre entreprise souhaite rationaliser ses fonctionnalités de gestion des identités et des accès également pour ses collaborateurs. Cette même plateforme d'identité client peut gérer tous ces types d'utilisateurs de façon fluide.

Une plateforme vous permet également d'exploiter des solutions de pointe dans le cadre de vos différents cas d'usage ou selon les besoins de pile technologique — qu'elles soient on-premise ou dans le cloud. Ainsi, vous pouvez utiliser les outils les plus performants du marché plutôt que d'être obligé d'opter pour des solutions médiocres proposées dans des offres packagées. Dans cette optique, choisissez une solution d'identité client avec un catalogue étendu de préintégrations prenant en charge les principaux services et applications de votre pile technologique, telles que :

- » API gateways
- » Détection des bots
- » Intégrateurs de données clients

- » Vérification d'identité
- » IaaS (Infrastructure-as-a-Service)
- » Gestion des accès à privilèges (PAM)
- » Analyses de sécurité

En outre, pour permettre à vos équipes de créer des workflows automatisés pour vos technologies clés sans devoir écrire de code personnalisé, privilégiez les solutions incluant des connecteurs no-code.

Enfin, votre solution doit assurer une intégration facile via des API, des SDK et des hooks. Avec les inline hooks, vos développeurs peuvent modifier les processus de gestion des identités clients en cours avec une logique personnalisée et des données provenant d'une source externe. Les event hooks quant à eux, à l'instar des webhooks, envoient en temps réel des événements d'identité client à un système en aval via une méthode HTTP POST. La figure 5-1 montre un exemple d'inline hook incorporé et d'event hook.

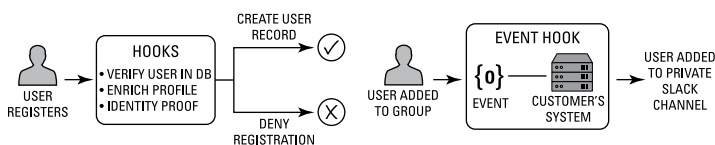


Figure 5-1. Exemple d'inline hook (à gauche) et d'event hook (à droite).

Établir une infrastructure fiable

Un atout majeur d'une solution d'identité client avancée est qu'elle est proposée en tant que service. En d'autres termes, vous n'avez plus l'obligation d'acheter et de maintenir l'infrastructure nécessaire pour bénéficier de l'évolutivité, de la fiabilité et de la sécurité dont vous avez besoin dans l'économie numérique actuelle, caractérisée par des changements rapides. Plus précisément, optez pour une solution présentant les caractéristiques suivantes:

- » **Évolutivité** – Votre solution doit pouvoir évoluer en fonction des besoins présents et futurs de l'entreprise. Votre système ne doit pas se transformer en goulet d'étranglement ou tomber en panne lorsque vos applications deviennent

populaires et que la demande explose. En outre, évitez d'avoir à remplacer votre fournisseur d'identité client s'il est incapable de tenir le rythme de votre croissance. Recherchez une solution d'identité client qui peut s'adapter à des centaines de milliers de demandes d'authentification par minute, et un fournisseur qui investit massivement dans sa solution et innove en permanence.

- » **Fiabilité** – Recherchez un partenaire d'identité client qui garantit la disponibilité la plus élevée et tient ses promesses. Les temps d'arrêt génèrent des pertes de revenus, nuisent à l'image de marque et peuvent faire fuir vos clients à cause d'une expérience médiocre et des évaluations négatives qui en résultent. Inutile d'acquérir les meilleurs produits si vos clients ne peuvent pas y accéder !
- » **Sécurité** – Choisissez un partenaire d'identité client qui propose une protection contre les attaques par credential stuffing, utilisant des identifiants compromis ou volés. Les attaques basées sur les identifiants s'appuient sur des informations d'identité faibles, trop souvent utilisées ou volées, qui servent à usurper l'identité d'utilisateurs légitimes ou à prendre le contrôle de comptes. Par exemple, les attaques par credential stuffing exploitent des noms d'utilisateur et mots de passe volés lors de brèches de données, capturés au cours de campagnes de phishing ou obtenues sur des forums en ligne. Les cybercriminels utilisent ensuite des outils automatisés pour les tester sur d'autres services en ligne. Les attaques par force brute et le password spray consistent à tester systématiquement ou automatiquement des mots de passe faibles ou trop utilisés, souvent en exploitant un ensemble connu de noms d'utilisateurs.



RAPPEL

Votre solution d'identité client a un impact direct sur l'expérience client et sur votre entreprise. Ce n'est pas votre fournisseur d'identité client que vos clients tiendront responsable de leurs problèmes d'évolutivité, de fiabilité et de sécurité, c'est vous. Si vous ne parvenez pas à répondre à leurs attentes, ils se tourneront vers la concurrence. Vous devez donc nouer une collaboration avec un partenaire qui possède une longue expérience dans la création de solutions d'identité client hautement évolutives, fiables et sécurisées, à même de vous faire gagner la confiance des clients.

Garantir votre leadership

Enfin, lorsque vous évaluez les différentes solutions d'identité client sur le marché, menez les vérifications nécessaires. La gestion des identités clients est un cheminement continu. Pour cette raison, vous avez besoin d'un partenaire qui s'engagera à assurer votre réussite à long terme, et pas un fournisseur qui vous vendra son produit et continuera sa route. Les attentes des consommateurs évoluent en permanence, tout comme les menaces de sécurité, les exigences réglementaires et les innovations technologiques. Pour savoir si un partenaire potentiel est un leader du marché, vérifiez par exemple s'il répond aux critères suivants :

- » Il est **validé par des tiers indépendants** via des rapports d'analystes et des certifications tels que :
 - Rapport SOC 2 type I et type II
 - Certification STAR niveau 2 de la CSA (Cloud Security Alliance)
 - ISO 27001:2013 et ISO 27018:2014
- » Il est **conforme à différentes exigences réglementaires**, comme le RGPD (règlement général sur la protection des données) de l'Union européenne et la loi HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis.
- » Son **expertise est validée par des références et témoignages de clients** similaires à votre entreprise en termes de secteur d'activité, de taille et d'emplacement géographique, et que vous pouvez contacter directement.
- » Il **offre une solution évolutive** appuyée par une solide expérience en termes d'innovation, des roadmaps produits, un rôle moteur dans le secteur, et une participation à des communautés de développeurs et à des groupes pour l'établissement de normes.

- » Cartographie du parcours de maturité de l'identité client
- » Les bases pour démarrer
- » Automatisation des opérations pour assurer la croissance et l'évolutivité
- » Optimisation de l'expérience client sans compromettre la sécurité
- » Viser l'excellence

Chapitre 6

Exprimer tout le potentiel de l'identité client en accord avec vos besoins métier

Le chapitre 5 décrit les critères à prendre en compte dans le choix d'une solution d'identité client avancée. Mais par où commencer ? Votre entreprise est unique, et vous devez adopter la solution qui correspond exactement à vos besoins spécifiques. Ce chapitre vous explique où et comment démarrer votre parcours de maturité en matière de gestion des identités et des accès clients.

Le parcours de maturité de l'identité client

Quel que soit le stade auquel votre entreprise est arrivée dans le parcours de maturité de l'identité client, des défis l'attendent. Nous allons analyser ce parcours qui s'articule en quatre stades : premiers pas, automatisation, intelligence et continuité (voir la figure 6-1).

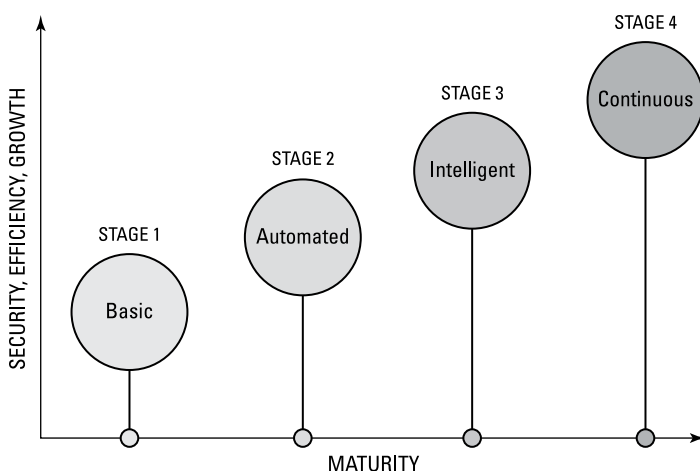


Figure 6-1. Où se trouve votre entreprise sur la courbe de maturité de l'identité client ?

À chaque stade du parcours de maturité, des actions précises vous permettront d'établir une gestion continue des identités et des accès clients. Les sections suivantes examinent les divers stades de façon plus approfondie, et ce qu'ils signifient pour votre entreprise.

Premiers pas: développer ou acheter ?

Votre entreprise souhaite commercialiser un nouveau produit et veut vérifier sa pertinence sur le marché. Imaginons par exemple qu'elle veuille créer une nouvelle application pour ses clients

et souhaite la lancer aussi vite que possible. Votre application est tout au début de son cycle de développement et vous devez démontrer sa viabilité. Vous disposez d'une équipe limitée, dont la priorité est de concevoir, développer et valider le business case de l'application. Différents compromis potentiels se présentent à vous.

D'un côté, vous avez des objectifs comme :

- » Lancer rapidement un produit minimum viable devant intégrer une fonctionnalité basique de gestion des identités.
- » Présenter votre produit à des clients potentiels.
- » Prouver que votre application résoudra un problème pour vos clients.

De l'autre côté, vous rencontrez différents défis :

- » Vous devez commercialiser votre produit et en proposer des itérations à mesure que vous en obtenez des retours.
- » Différents problèmes de sécurité de base peuvent faire dérailler la totalité du projet.
- » Vous disposez de ressources d'ingénierie limitées et ne savez pas vraiment où intégrer la gestion des identités dans votre infrastructure.

C'est le premier stade du parcours de maturité de l'identité client, où vous devez décider si vous allez utiliser votre temps limité et vos précieuses ressources pour créer votre propre solution d'identité client ou si vous allez collaborer avec un fournisseur tiers.

Comme nous l'expliquons dans le chapitre 3, le développement et la gestion d'outils internes vont accaparer vos développeurs et ingénieurs, qui ne pourront plus se consacrer aux produits stratégiques de votre entreprise. Il serait donc plus simple de profiter d'une solution externe pour configurer rapidement les principales fonctionnalités d'identité client dont vous avez besoin : authentification, autorisation et gestion des utilisateurs. Cela vous permettrait également d'établir des bases solides pour offrir des accès sécurisés à vos clients, tout en utilisant vos développeurs de la façon la plus efficace possible.



D'après un sondage Harris Poll de Stripe.com, les développeurs passent en moyenne 17,3 heures par semaine à déboguer et à maintenir du code hérité et de mauvaise qualité. Avec une solution d'identité client avancée, vous pouvez accélérer le développement et limiter les efforts de maintenance à long terme, ce qui vous permet de vous concentrer sur vos activités stratégiques.

Une fois le premier stade terminé, vous avez intégré des fonctionnalités cruciales de sécurité des identités dans votre application et vous l'avez lancée avec succès. La prochaine étape est d'étendre votre offre de produits pour répondre aux demandes d'une clientèle de plus en plus large.

Automatisation : centraliser et mettre à l'échelle

Félicitations ! Votre application rencontre un franc succès et vous souhaitez désormais développer de nouveaux produits. Vous recrutez, et vous disposez désormais d'un directeur technique ou d'un directeur produit ou ingénierie qui dirige votre projet. Cependant, ce nouveau stade s'accompagne de nouveaux défis. Par exemple, votre clientèle en pleine expansion exige des fonctionnalités plus sophistiquées ou adaptées à un environnement d'entreprise, que vous n'avez ni le temps, ni l'expérience de développer. Vous devez donc prioriser vos initiatives pour adapter vos opérations et poursuivre votre croissance.

Vous pourriez envisager de développer les fonctionnalités d'identité client en interne en raison de leur importance critique, mais les objectifs prioritaires à cette étape seront plutôt de créer et de lancer de nouveaux produits, afin de continuer à étoffer votre clientèle.

Vous êtes arrivé au stade Automatisation, où une solution d'identité client externe appropriée vous aidera de différentes façons :

- » En vous libérant de la gestion des identités des clients externes et du risque associé. Vos utilisateurs finaux doivent pouvoir se connecter aux fournisseurs d'identité existants et vous devriez pouvoir déléguer l'authentification à des annuaires Active Directory ou LDAP. Votre entreprise peut ainsi centraliser la gestion des utilisateurs et la mettre à l'échelle sans effort.

- » En utilisant des normes d'authentification modernes comme OpenID Connect, OAuth et SAML (Security Assertion Markup Language) pour adopter automatiquement les dernières pratiques de sécurité et d'identité sans devoir rattraper vos retards permanents.
- » En vous conformant à différentes réglementations, comme le RGPD (Règlement général sur la protection des données) de l'Union européenne et la loi CCPA (California Consumer Privacy Act) aux États-Unis.
- » En automatisant des processus tels que le provisioning et le déprovisioning grâce à la gestion du cycle de vie des clients.
- » En renforçant la sécurité à mesure que vous mettez vos systèmes à l'échelle et détectant automatiquement les mots de passe vulnérables ou compromis.
- » En offrant à vos clients des méthodes modernes pour réinitialiser leurs mots de passe ou s'authentifier (par SMS, messages vocaux, e-mail ou mots de passe à usage unique), et en gérant ces politiques de sécurité depuis une console d'administration centralisée.

La finalisation du stade Automatisation signifie que vous avez étendu la portée de vos produits et amélioré la sophistication de vos fonctionnalités de gestion des utilisateurs, de mise en conformité et de sécurité. Cependant, comme vos systèmes évoluent sans cesse, vous devez investir dans des protections plus fortes et dans de nouvelles fonctionnalités pour optimiser davantage encore l'expérience client.

Intelligence : optimiser sans compromis

À ce stade, votre entreprise est bien positionnée pour être leader du marché. Pour continuer sur sa lancée, elle doit optimiser son offre de produits, sans sacrifier les exigences complexes en matière d'identité de vos parties prenantes internes (par exemple, les équipes produit, ingénierie et marketing) qui tentent d'offrir une expérience client fluide et sécurisée à grande échelle.

Une solution d'identité client avancée vous aidera de diverses façons à trouver le bon équilibre et à améliorer votre infrastructure afin qu'elle prenne en charge les API et les microservices :

- » En offrant une expérience d'onboarding sophistiquée avec un niveau d'assurance plus élevé via des fonctionnalités de vérification des identités et des comptes.
- » En assurant une expérience client fluide sans compromettre la sécurité, avec des solutions telles que l'AMFA (une couche d'intelligence adaptative qui exploite des informations contextuelles et comportementales pour analyser les risques et exiger un facteur supplémentaire le cas échéant), l'authentification sans mot de passe (par exemple, via des magic links par e-mail et WebAuthn) et le progressive profiling qui collecte les attributs des profils utilisateurs au fil du temps.
- » En respectant les exigences de conformité les plus récentes en termes de confidentialité et de sécurité via la consolidation de la gestion des données et du cycle de vie des utilisateurs au sein d'un système de connexion centralisé.
- » En optimisant toutes ces opérations via l'extension des fonctionnalités d'identité client à votre pile technologique au moyen de préintégrations ou de workflows personnalisés, et via des technologies de pointe (par exemple, le blocage des bots, la gestion de la relation client et les outils d'analyse marketing).

À ce stade, votre application offre à vos clients une protection forte, éventuellement sans mot de passe. Votre utilisation des données clients et la façon dont vous les stockez sont perpétuellement personnalisables et 100 % conformes avec les réglementations relatives à la protection de la confidentialité. Avec des intégrations de pointe, votre système de protection des identités est rigoureux, et vous pouvez détecter et atténuer les risques proactivement. Les clients utilisent vos services avec confiance et facilité, et vous êtes bien positionné pour explorer d'autres fonctionnalités avancées.

Continuité : devenir un leader et une référence du secteur

C'est le dernier stade de la courbe de maturité de l'identité client. Seuls les leaders du marché, c'est-à-dire les entreprises qui ont réalisé leur transformation digitale, y parviennent. Ils disposent d'une équipe interne dédiée à l'identité client, qui prend en charge une stratégie omnicanale permettant d'optimiser la sécurité et

l'expérience client. Ces leaders se démarquent de la concurrence, car ils ont compris que l'identité est un parcours continu qui exige une stratégie à long terme.

En effet, pour rester à la première place, il faut établir en permanence de nouveaux standards d'excellence. À ce stade, votre solution d'identité client fait bien plus que d'assurer des connexions fluides et sécurisées. Elle vous aide aussi à :

- » Effectuer le suivi des clients sur tous les canaux (plateformes web et mobiles comme magasins physiques) afin d'en obtenir une vue à 360 degrés et de leur offrir une expérience omnicanale personnalisée ;
- » Implémenter des autorisations granulaires et basées sur les risques afin d'optimiser le contrôle des accès et d'éviter toute exposition des données, de répondre à des normes sectorielles strictes (comme FAPI) et de limiter les points de friction. Vous pouvez définir des facteurs de risque pour des catégories comme les réseaux, les lieux, les terminaux et les types de transactions. Un score de risque peut être calculé de façon dynamique ou déclenché par des conditions spécifiques (par exemple des horaires et des événements utilisateurs) ;
- » Automatiser l'orchestration de la sécurité et l'intervention en cas d'incident au moyen de workflows flexibles, et limiter le temps et les efforts passés à gérer les politiques d'identité et de sécurité à l'aide de l'intelligence artificielle et du machine learning.



Que vous développiez un produit pour la première fois ou que vous soyez un leader du marché bien établi, l'intégration de l'identité client dans votre roadmap produits est cruciale. Savoir à quel stade vous vous trouvez sur la courbe de maturité de l'identité client signifie que votre entreprise peut surveiller ses performances et identifier les domaines à prioriser afin de gagner un avantage concurrentiel.

- » Des expériences qui favorisent l'engagement
- » Une sécurité renforcée qui suscite la confiance en votre marque
- » Conformité réglementaire et protection de la vie privée
- » Prise en charge d'architectures et de cas d'usage de plus en plus complexes

Chapitre 7

Imaginer l'avenir de l'identité client

Dans ce chapitre, nous nous tournons vers l'avenir en explorant quatre tendances qui vont façonner l'identité client et aider votre entreprise à prospérer.

Renforcer l'engagement des clients

Les entreprises orientées clients doivent constamment innover et améliorer les interactions des utilisateurs avec leur marque afin d'augmenter leur engagement et de tirer parti d'une valeur vie maximale. Il est donc tout à fait logique que l'une des principales tendances qui vont déterminer l'avenir de l'identité client soit l'amélioration de l'engagement des clients et l'accélération des délais de rentabilisation. Car au final, si vous créez un nouveau produit, c'est pour que les utilisateurs s'en servent. Leur offrir une expérience client optimale est donc crucial pour établir des relations positives avec eux.



CONSEIL

Une solution d'identité client avancée conçue pour rester pertinente à long terme vous aidera de bien des manières à renforcer l'engagement de vos clients :

- » **En adaptant la quantité d'informations que les clients doivent saisir en fonction du moment, de la personne et du stade atteint sur le parcours client.** Au lieu de demander à de potentiels nouveaux clients de fournir des tonnes d'informations au cours d'un processus d'enregistrement interminable, utilisez des innovations telles que le progressive profiling pour limiter les points de friction et améliorer votre taux de conversion.
- » **En présentant à vos clients des contenus adaptés à leur réalité, dans la langue et le format qu'ils préfèrent.** Établissez des relations de confiance en vous adressant à vos clients dans leur langue d'expression, et gérez la traduction et la personnalisation séparément.
- » **En permettant à votre entreprise d'offrir une image de marque cohérente à chaque interaction, afin de nouer une relation avec les clients et de susciter leur confiance.** Incorporez vos éléments de marque à chaque étape du parcours d'identification des clients. Par exemple, permettez leur d'utiliser votre propre application d'authentification multifacteur (MFA) via des kits SDK ou des API.



RAPPEL

Créer une expérience optimale est l'une des façons les plus rapides de susciter l'engagement des clients, et des clients très engagés sont plus susceptibles d'acheter davantage de produits et plus souvent.

Renforcer la sécurité

Afin d'établir des relations de confiance entre vos clients et votre marque, une solution d'identité client avancée doit atteindre le juste équilibre entre sécurité et expérience client. Les menaces de cybersécurité continuent d'évoluer, devenant de plus en plus sophistiquées et dangereuses. Dans ce contexte, il peut être tentant de faire abstraction de ce fragile équilibre pour appliquer des mesures de sécurité fortes, au détriment de la facilité d'utilisation.

Pendant, il est tout à fait possible de mettre en place des protections appropriées, à la fois pour l'entreprise et les clients, en offrant aux utilisateurs le niveau de sécurité qui leur convient

et en ajoutant des contrôles de sécurité qui n'impliquent pas de saisir directement des informations. L'objectif n'est pas d'accumuler les mesures de sécurité, mais plutôt de rendre la sécurité plus efficace.



Plutôt que d'implémenter les options de sécurité les plus strictes et innovantes disponibles dans les solutions d'identité client avancées, les entreprises doivent appliquer le bon niveau de sécurité au bon moment, en proposant des politiques flexibles et en maintenant une expérience aussi simple que possible.

Pour bénéficier d'une sécurité efficace à long terme et susciter en toute simplicité la confiance en votre marque, suivez ces quelques conseils :

- » **Appliquez le niveau de sécurité adapté au stade approprié du parcours client.** Même les entreprises possédant des milliers d'applications orientées clients peuvent simplifier l'expérience en demandant aux utilisateurs de saisir seulement le minimum d'informations (il s'agit d'un point de friction) au stade approprié du parcours client (par exemple pendant l'enregistrement). Ainsi, vous pouvez appliquer un processus d'authentification multifacteur (MFA) uniquement lorsque c'est nécessaire, par exemple quand les clients se connectent depuis un lieu suspect ou un terminal inconnu.
- » **Établissez des politiques de sécurité différentes pour chaque application afin d'atteindre l'équilibre idéal entre expérience fluide et sécurité.** Par exemple, les applications qui servent à s'enregistrer et à réaliser des achats exigent un niveau de sécurité plus élevé que celles qui permettent juste de vérifier le statut d'une commande, même s'il s'agit du même utilisateur et de la même marque.
- » **Permettez aux utilisateurs finaux de décider par eux-mêmes s'ils souhaitent activer la MFA.** Au lieu d'obliger vos clients à se soumettre à un processus d'authentification multifacteur (MFA), laissez-leur le choix. Bien que la MFA devienne de plus en plus courante, de nombreuses personnes continuent à trouver ce processus ennuyeux. Vous pouvez donc choisir de surveiller d'autres facteurs de risque (le terminal, le lieu ou le réseau) sans demander à vos utilisateurs de saisir des informations.
- » **Permettez à vos clients de récupérer leurs comptes via n'importe quel facteur.** Une pratique toujours gagnante est d'offrir des fonctionnalités flexibles en libre-service (par exemple, l'authentification par e-mail, par SMS, via un

mot de passe à usage unique, etc.) grâce auxquelles vos clients pourront récupérer leurs comptes ou réinitialiser leurs mots de passe sans avoir besoin de contacter le support.

- » **Étendez l'identité client à chaque point de contact pour intégrer des services tiers.** Utilisez des technologies spécialisées pour ajouter des fonctionnalités et améliorer l'expérience client à chaque point de contact au fil de leur parcours.

Protéger la confidentialité

Les réglementations de protection de la confidentialité, comme le RGPD et la loi CCPA, ont déjà un impact sur les activités des entreprises. Par ailleurs, comme les clients exigent de plus en plus de contrôle sur leurs informations personnelles, de nouvelles réglementations sont régulièrement promulguées partout dans le monde. Pour maintenir la confiance, les entreprises doivent s'adapter. Cependant, la confidentialité est une notion complexe qui ne se résume pas à demander l'accord des clients sur l'utilisation de leurs données. Du point de vue de l'identité client, les futures fonctionnalités devront répondre à ces trois cas d'usage principaux :

- » **Gestion des préférences:** traitement et stockage des données clients
- » **Gestion de la confidentialité:** partage des informations des clients
- » **Gestion de la conformité:** repérage et suppression potentielle des données à caractère personnel

Ces fonctionnalités peuvent être fournies prêtes à l'emploi dans une solution d'identité client ou via des intégrations avec des fournisseurs tiers spécialisés dans les cas d'usage de gestion de la confidentialité et du consentement.

Si vous protégez efficacement la confidentialité de vos utilisateurs, vous gagnerez la confiance de vos clients et assurerez votre conformité de bout en bout. Au final, c'est votre entreprise qui en bénéficiera.



CONSEIL

Pour aborder plus facilement le paysage réglementaire complexe actuel et futur, adoptez une solution d'identité client qui gèrera à votre place les données à caractère personnel de vos clients en matière de préférences, de confidentialité et de conformité.

Gérer la complexité

La complexité caractérise la vie des entreprises: elles doivent développer, tester et lancer des applications cloud-native modernes pour des clients exigeants ; fédérer des référentiels d'identités externes et fragmentés sur tous les portails de leurs partenaires; et maintenir les solutions héritées jusqu'à la finalisation d'une transformation digitale qui peut prendre plusieurs années. Cette complexité signifie qu'une solution d'identité client ne permet plus simplement aux clients de se connecter à une application ou à un site web.

Elle doit aussi assurer la flexibilité et la croissance de l'entreprise. En particulier, elle doit pouvoir :

- » Prendre en charge à grande échelle une architecture multiorganisation comportant de nombreux environnements de test, de préproduction et de production ;
- » Traiter un environnement hybride composé d'applications cloud avancées et de produits on-premise tout en assurant la séparation des données ;
- » Offrir une prise en charge étendue des API et une administration intuitive entre toutes les organisations ;
- » Aider à organiser des systèmes de gestion des identités fragmentés.

- » Checklist pour l'implémentation de l'identité client
- » Identification initiale des exigences techniques et métier
- » Choix d'une solution d'identité client adaptée à votre entreprise
- » Identité client et innovation continue
- » Avantage concurrentiel grâce à une expérience client fluide

Chapitre 8

Dix considérations liées à l'identité client

Ces dix considérations vous aideront à choisir et à implémenter la solution d'identité client adaptée à votre entreprise:

- » **Prenez le temps de cerner les points de friction que subissent vos clients et vos équipes internes.** Les clients sont-ils gênés par un processus d'enregistrement trop long ? Avez-vous subi une brèche de sécurité ? Vos initiatives de transformation digitale sont-elles ralenties ?
- » **Définissez votre expérience client idéale.** Quelle expérience souhaitez-vous offrir à vos clients lorsqu'ils interagissent avec votre marque ? Souhaitez-vous leur permettre d'accéder à toutes vos applications via une expérience de connexion unique et à votre image ? Quels canaux pensez-vous utiliser ?
- » **Déterminez vos spécifications de sécurité.** Comment offrez-vous actuellement une expérience d'accès sécurisée ? Quelle expérience souhaitez-vous proposer à l'avenir ?

À quelles réglementations de sécurité et de protection de la confidentialité devez-vous vous conformer ?

- » **Établissez vos objectifs métier.** Quels sont vos objectifs commerciaux ? L'expansion internationale, le lancement d'un nouveau produit ? Dans quels délais ?
- » **Listez et analysez vos besoins en matière d'identité client.** Classez vos exigences (métier, expérience utilisateur, sécurité) par ordre de priorité, depuis les nécessités absolues jusqu'aux options facultatives. Faites-les coïncider avec vos besoins internes et déterminez comment trouver le meilleur compromis.
- » **Estimez le coût d'opportunité du développement en interne par rapport à l'achat.** La création et la maintenance d'une solution d'identité client maison est difficile (et inutile) : il est préférable de se concentrer sur son cœur de métier. Pour appréhender tout ce qu'implique la création en interne d'une solution d'identité client, reportez-vous au chapitre 3.
- » **Confiez la gestion des identités clients à un expert externe (pour obtenir une solution de qualité).** Avec l'aide de ce livre, identifiez l'expert en identité client le plus approprié pour votre entreprise. Recherchez un partenaire de confiance ayant une solide expérience en la matière, qui sera capable de répondre à vos besoins actuels et futurs.
- » **Déployez une expérience client fluide.** Une fois que vous avez choisi votre solution d'identité client avancée, vous pouvez la déployer rapidement et à grande échelle sur l'ensemble de vos applications, sites web et portails orientés clients, afin d'offrir des expériences fluides et sécurisées.
- » **Libérez votre capacité d'innovation en progressant dans la courbe de maturité de l'identité client.** Une solution d'identité client avancée s'accompagne d'une foule d'opportunités. Pour en savoir plus sur les possibilités qui s'offrent à vous au fil de la courbe de maturité de l'identité client, reportez-vous au chapitre 6.
- » **Concentrez-vous sur votre avantage concurrentiel.** Une solution d'identité client avancée peut représenter un facteur de différenciation qui aidera votre entreprise à acquérir une réputation reposant sur la confiance, l'innovation et l'excellence de l'expérience client.



okta

Identité client : notre guide répond à vos questions



bit.ly/OktaCIAudiobook

Écouter
le livre audio
maintenant

Créez des expériences clients fluides et sécurisées

Si vous avez déjà créé un compte sur un site web pour acheter des billets de concert, ou utilisé l'un de vos comptes de réseaux sociaux pour vous connecter à un nouveau site d'e-commerce, vous avez déjà interagi avec l'identité client. L'identité client offre une couche d'identité numérique qui peut s'intégrer aux applications, sites web et portails orientés clients. Dans ce guide, vous découvrirez comment l'identité client peut vous aider à offrir des expériences fluides et sécurisées à vos clients et partenaires.

À l'intérieur...

- Les principes fondamentaux de l'identité client
- Pourquoi l'identité client est cruciale
- Les risques du développement en interne d'une solution d'identité client
- En quoi consiste une solution d'identité client avancée
- Les fonctionnalités incontournables d'une solution d'identité client
- Comment une gestion des identités clients sur mesure peut aider votre entreprise à prospérer
- L'avenir de l'identité client



okta

Lawrence C. Miller travaille dans l'informatique depuis plus de 25 ans et a rédigé près de 200 ouvrages de la collection « Pour les nuls ». **Jeremie Certes** est Senior Product Marketing Manager chez Okta.

Consultez le site **Dummies.com™**

pour voir des vidéos, des exemples pas-à-pas ou des articles pratiques, ou pour vous procurer d'autres ouvrages de notre collection.

ISBN: 978-1-394-22821-8

Revente interdite



pour
les nuls®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.