UNE PUBLICATION

auth0

CIAM (Customer Identity & Access Management)

pour les nuls®

Pourquoi le CIAM est aujourd'hui plus important que jamais

Avantages d'une solution CIAM avancée

Critères d'une solution CIAM performante

Édition spéciale Auth0

Lawrence C. Miller

Jeremie Certes

À propos d'Auth0

Auth0, récemment acquis par Okta, propose une plateforme permettant d'authentifier, d'autoriser et de sécuriser l'accès pour les applications, les périphériques et les utilisateurs. Les équipes de sécurité et d'applications s'appuient sur la simplicité, l'évolutivité et l'expertise d'Auth0 pour rationaliser les identités à tous les niveaux. En protégeant plus de 4,5 milliards de transactions de connexion chaque mois, Auth0 sécurise les identités afin que les innovateurs puissent innover, et permet aux entreprises internationales d'assurer des expériences numériques fiables et optimales à leurs clients du monde entier.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

CIAM (Customer Identity & Access Management)

Édition spéciale Auth0

Lawrence C. Miller et Jeremie Certes

pour les nuls®

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

CIAM (Customer Identity & Access Management) pour les nuls® Édition spéciale Auth0

Publié par **John Wiley & Sons, Ltd.**, The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com

© 2022 de John Wiley & Sons, Ltd., Chichester, West Sussex

Siège social

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, Royaume-Uni

Tous droits réservés. 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 la loi du Royaume-Uni de 1988 relative au copyright (« Copyright, Designs and Patents Act ») l'autorise. Pour savoir comment demander l'autorisation à l'éditeur de réutiliser du contenu sous copyright, veuillez consulter notre site web 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. Auth0, Okta et le logo Auth0 sont des marques de commerce ou des marques déposées d'Okta, Inc. Toutes les autres marques appartiennent à leurs propriétaires 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 L'AUTEUR ONT FOURNI TOUS LES EFFORTS POSSIBLES DANS LA PRÉPARATION DE CE LIVRE, ILS NE FONT AUCUNE DÉCLARATION NI N'ACCORDENT AUCUNE GARANTIE QUANT À L'EXACTITUDE OU À L'EXHAUSTIVITÉ DU CONTENU DU PRÉSENT LIVRE ; EN PARTICULIER, ILS REJETTENT SPÉCIFIQUEMENT TOUTES LES GARANTIES, Y COMPRIS, SANS AUCUNE LIMITE, LES GARANTIES D'ADÉQUATION À UN USAGE PARTICULIER. LE PRÉSENT LIVRE EST VENDU ÉTANT ENTENDU QUE L'ÉDITEUR N'OFFRE PAS DE SERVICES PROFESSIONNELS, ET QUE NI L'ÉDITEUR, NI L'AUTEUR NE SERONT TENUS RESPONSABLES DES DOMMAGES DÉCOULANT DU CONTENU DU PRÉSENT LIVRE. LES LECTEURS QUI VEULENT OBTENIR UNE ASSISTANCE PROFESSIONNELLE OU L'AIDE D'UN EXPERT DOIVENT S'ADRESSER À UN PROFESSIONNEL COMPÉTENT.

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un livre *Pour les nuls* destiné à votre entreprise ou organisation, veuillez contacter 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 978-1-119-86657-2 (pbk); ISBN 978-1-119-86658-9 (ebk)

Imprimé en Grande-Bretagne

10 9 8 7 6 5 4 3 2 1

Remerciements de l'éditeur

Rédacteur : Jack Hyman

Chef de projet : Martin V. Minner

Directrice des acquisitions : Ashley Coffey

Directeur de la rédaction : Rev Mengle

Représentante du développement commercial : Molly Daugherty

Éditeur de production : Mohammed Zafar Ali

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Sommaire

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Introduction

Vous avez sans aucun doute déjà utilisé le CIAM (Customer Identity & Access Management) dans votre vie personnelle en qualité de client, 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 le CIAM au quotidien sur leurs applications, sites web et portails préférés.

Dans ce livre, vous découvrirez comment une solution CIAM avancée peut aider votre entreprise à offrir des expériences numériques sécurisées et fluides à ses clients et partenaires.

À propos de ce livre

CIAM (Customer Identity & Access Management) pour les nuls, Édition spéciale Auth0, comporte huit chapitres qui explorent les questions suivantes :

- Les concepts fondamentaux du CIAM (chapitre 1)
- Pourquoi le CIAM est plus important que jamais (chapitre 2)
- Pourquoi il n'est pas recommandé de développer un CIAM maison (chapitre 3)
- En quoi consiste une solution CIAM avancée et comment elle peut aider votre entreprise (chapitre 4)
- Les fonctionnalités incontournables d'une solution CIAM avancée (chapitre 5)
- Les atouts d'une solution CIAM adaptée à vos besoins métier (chapitre 6)
- L'avenir du CIAM (chapitre 7)
- Dix considérations liées au CIAM 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 livre dans l'ordre qui vous convient (même si nous déconseillons de le lire à l'envers).

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 la gestion des identités et des accès.

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://auth0.com/fr/ciam`.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

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

Chapitre 1
Qu'est-ce que le CIAM ?

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 CIAM. 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 un formulaire qu'à trouver ce dont on a besoin.

Ce chapitre explore les principes fondamentaux du CIAM, son fonctionnement, les effets négatifs d'une expérience CIAM médiocre, l'importance de ce type de solution pour vos clients et vos applications, et les fonctionnalités que tout CIAM de qualité se doit de posséder.

Qu'est-ce que le CIAM ?

Même si l'acronyme lui-même ne vous est pas familier, vous utilisez en fait le CIAM au quotidien : lorsque vous accédez à des applications

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

mobiles, lorsque vous vous inscrivez à un nouveau service en ligne ou lorsque vous vous authentifiez sur votre site préféré. Le CIAM offre une couche d'identités numérique qui peut s'intégrer aux applications, sites web et portails qui sont accessibles au grand public. C'est lui 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, le CIAM ne se résume pas à assurer la connexion et l'authentification des utilisateurs : il se charge également du processus d'enregistrement et de création de comptes. En d'autres termes, il intervient sur la totalité du parcours client.

Pour cette raison, une expérience CIAM médiocre peut faire fuir vos clients au profit de concurrents qui offrent des expériences plus fluides et intuitives. Mais comment définit-on la (mauvaise) qualité d'une expérience CIAM ?

Qu'est-ce qu'une mauvaise expérience CIAM ?

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 y a fort à parier que vous avez déjà vécu une mauvaise expérience CIAM dans vos transactions personnelles et professionnelles. Voici quelques exemples de points de friction liés au CIAM, 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 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

En revanche, une bonne expérience CIAM 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

Dans le cas d'une mauvaise expérience CIAM, les points de friction inutiles jalonnent le parcours client, comme un processus d'enregistrement trop long et intrusif, ou la nécessité d'appeler un service client pour réinitialiser un mot de passe. Un CIAM mal conçu oblige en outre vos développeurs à créer des intégrations et des connexions personnalisées pour vos nouvelles applications, ce qui ralentit leur mise sur le marché. 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, un CIAM de mauvaise qualité 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 CIAM devenir des points de tension pour vos clients. Faites de votre CIAM 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 avec vos clients, adoptez une solution CIAM avancée. La gestion des identités et des accès 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 CIAM 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).

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 CIAM 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 accèdent 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 ils doivent pouvoir retrouver facilement les mêmes fonctionnalités, quelle que soit la ressource utilisée.

Principales fonctionnalités

Les trois principales fonctionnalités d'un CIAM efficace sont l'authentification, l'autorisation et la gestion des utilisateurs. Dans le cadre du CIAM, 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 des ressources.

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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

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

Chapitre 2
Pourquoi le CIAM est plus important 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 : la 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 et la confidentialité, et la transformation digitale sont autant de facteurs qui motivent et accélèrent tout à la fois la nécessité de déployer une solution CIAM de pointe, maintenant plus que jamais.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Répondre à la demande en matière d'expérience client avancée

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, 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

Un article du site Entrepreneur.com (« Vroom! Why Website Speed Matters », 19 mai 2017), citant une analyse Kissmetrics, indique que « 47 % des consommateurs attendent d'une page web qu'elle se charge en deux secondes ou moins » et que « 40 % abandonnent un site web dont le chargement prend plus de trois secondes ». Sachant cela, vous croyez réellement que vos clients attendront sagement la fin d'un processus de connexion qui prend plusieurs minutes ?

Une solution CIAM avancée 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 (en matière de consentement, notamment) 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 CIAM moderne, vous pouvez proposer une expérience fluide à vos clients, avec des innovations telles que l'authentification sans mot de passe (via reconnaissance faciale ou empreinte digitale, par exemple), et ce, quel que soit le terminal qu'ils utilisent.

RAPPEL

Les solutions de gestion des identités et des accès collaborateurs (IAM) et clients (CIAM) sont des technologies 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.

Cultiver la confiance des clients

La réussite d'une entreprise repose en bonne partie sur sa capacité à gagner, puis à conserver, 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

est un impératif absolu. S'ils ne vous font pas confiance, ils passeront vite à la concurrence.

AVERTISSEMENT

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 actuelle 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 divulgation, 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 CIAM 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 des technologies innovantes telles que l'authentification multifacteur (MFA) et l'authentification sans mot de passe, 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **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 récentes, 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 CIAM 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 cinq 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.

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).

RAPPEL

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 CIAM avancée qui les aide à mener leur transformation digitale, en particulier :

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **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, alliée 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 CIAM avancée conçue dans le cloud, vos développeurs pourront très facilement intégrer des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs dans les applications qu'ils créent, et se concentrer davantage sur les activités stratégiques.


TECHNIQUE

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. Comme un CIAM avancé est capable de contrôler les API et d'en sécuriser l'accès, l'entreprise peut étendre ses activités basées sur les API en toute sécurité.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- **Création d'expériences clients fluides et sécurisées**
- **Utilisation judicieuse des ressources limitées de votre équipe de développement**
- **Intégration du CIAM à la pile technologique pour plus de fiabilité et une mise sur le marché accélérée**
- **Calcul du coût total du développement d'un CIAM par rapport à son achat**

Chapitre 3
Création d'un CIAM : attention, danger

Le chapitre 2 a détaillé les raisons pour lesquelles une solution CIAM 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. C'est le but de ce chapitre.

Expérience client vs sécurité et conformité : un équilibre difficile

Développer une solution CIAM 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 :

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **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 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 optimale grâce à votre CIAM, vous devez d'abord définir les exigences de vos clients, et elles sont nombreuses. De plus, elles peuvent différer très fortement d'une personne à l'autre : ce qui enchante un consommateur en rebutera un autre.

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

LE CIAM, 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 nom-

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

breuses relations B2B, une entreprise vend et l'autre achète. De nombreuses exigences de gestion des identités et des accès clients 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.

Si vous envisagez sérieusement de développer votre propre CIAM, 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, ou AMFA (qui demande 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 CIAM, vous ne manquerez pas d'attirer les pirates. Vous allez devoir faire en sorte que votre CIAM maison ne remplace pas les utilisateurs en tant que « 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 le CIAM 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 maintenir 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, 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 CIAM maison ne respecte pas ces différentes réglementations, votre entreprise risque gros en termes d'amendes et autres sanctions.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Enfin, toujours dans le cas où vous persistez à vouloir développer votre propre CIAM, 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 CIAM, 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 CIAM sécurisées offrant une expérience client optimale, des

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

capacités pointues de sécurité et de protection de la confidentialité, et une conformité réglementaire en continu, 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'un CIAM. 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 ?

RAPPEL

Le développement d'un CIAM maison implique d'écrire énormément de code personnalisé. Or, selon le Top 10 de l'*Open Web Application Security Project (OWASP)* (`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 onéreuse) 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 CIAM :

- **Nécessité d'une évolutivité à grande échelle :** les clients veulent pouvoir accéder de façon sécurisée et fluide à vos applications mobiles, sites web 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 ?

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **Intégration avec votre pile technologique :** pour que vous puissiez étendre les fonctionnalités et maximiser le ROI de votre solution CIAM, 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 mise sur le marché :** 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 CIAM 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 un CIAM 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 un CIAM 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 d'un CIAM maison est difficile (et inutile), ne faites pas non plus de compromis lors de votre achat. Dans le chapitre 4, vous allez découvrir comment une solution CIAM avancée peut aider votre entreprise. Le chapitre 5 vous expliquera les fonctionnalités que vous devez attendre d'un CIAM performant.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- En quoi consiste une solution CIAM avancée
- Les atouts du modèle en plateforme
- Une infrastructure de services sécurisée, fiable et évolutive
- Étude de cas d'usage et témoignages clients

Chapitre 4
Avantages d'une solution CIAM avancée pour votre entreprise

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

Qu'est-ce qu'une solution CIAM avancée ?

Une solution CIAM avancée fournit une couche d'identités 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 en leur offrant une expérience utilisateur fluide, en raccourcissant les délais de mise sur le marché, en gérant de façon centralisée les politiques d'identification et d'accès, et en renforçant la sécurité à l'échelle d'Internet.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Des expériences utilisateurs optimales

Pour proposer des expériences fluides, vous devez connaître et comprendre vos clients. Avec une solution CIAM 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 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 externes 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.

TECHNIQUE

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.

Une mise sur le marché accélérée

Comme les solutions CIAM avancées incluent 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, vous pouvez accélérer vos délais de mise sur le marché. 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 pratiquement sans programmation, 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 CIAM dans les expériences clients, plutôt que de les créer de A à Z, ce qui accélère la mise sur le marché.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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.

AVERTISSEMENT

Gérer les identités et les accès 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 CIAM 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 CIAM 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 en plateforme

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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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. Un CIAM développé en interne sera certainement créé par différentes équipes produits : une consacrée au cas d'usage interne, l'autre au partenaire externe. 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 CIAM avancée basée sur une plateforme unique assure une approche IAM cohérente pour tous les utilisateurs finaux et optimise les synergies.

Par ailleurs, le modèle en plateforme indépendante et neutre permet également d'étendre les capacités CIAM 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 pré-intégrations 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 CIAM 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 non 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Une solution CIAM 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 CIAM avancée 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.

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 de solutions CIAM avancées 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

Un CIAM 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.

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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 CIAM 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.

MAJOR LEAGUE BASEBALL

Les supporters de la Major League Baseball (MLB) ne sont plus cantonnés aux stades et à leur salon. Ils utilisent désormais une multitude de technologies, y compris les terminaux mobiles, le live streaming et les applications des stades, pour soutenir leurs équipes de baseball préférées. La MLB a décidé de moderniser son environnement numérique pour offrir une expérience omnicanale fluide et capable de monter en charge pour répondre à la demande de millions de fans.

Comme elle ne disposait que de neuf mois pour développer sa nouvelle plateforme grand public, qui devait être prête avant le lancement de la saison 2019, la MLB a continué sa collaboration avec Okta, après la réussite de l'implémentation de solutions IAM Okta dans tous ses clubs de baseball. En collaboration étroite avec Okta, elle est parvenue à migrer des millions d'utilisateurs à partir de sa base de données interne. Pour garantir la capacité des systèmes de la MLB à faire face aux pics de trafic, des tests de performance ont été menés en lançant jusqu'à 138 000 demandes authentifiées par minute.

La nouvelle plateforme a été inaugurée sans heurts le jour de l'ouverture de la saison 2019, et des dizaines de millions de supporters profitent maintenant des applications de la MLB sur leurs terminaux préférés, où qu'ils se trouvent et à tout moment.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

ALBERTSONS

Albertsons Companies compte plus de 30 millions de clients chaque semaine, via plus de 20 marques. L'évolution des exigences des consommateurs constituait un défi inédit pour ce groupe de grande distribution à la réputation bien établie. Il lui fallait proposer une expérience fluide et homogène tout en restant fidèle à l'image et à l'apparence de ses différentes marques.

Albertsons souhaitait notamment éliminer les comptes clients en double. Par exemple, si un client avait créé un compte pour deux marques différentes, Albertsons devait fusionner ces comptes et les données associées, sans perturber l'expérience des clients. Le groupe avait donc besoin d'une solution qui faciliterait l'unification de ses données clients sur toutes ses marques et applications.

Grâce à Okta, Albertsons a pu simplifier son processus de migration des utilisateurs. Le groupe est désormais à même d'offrir une expérience personnalisée et fluide à des millions de clients sur ses différentes marques, tout en poursuivant sa croissance au fil de l'acquisition de nouvelles enseignes.

Intégration des identités d'entreprise

Avec un CIAM avancé, 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

HPE GREENLAKE

En 2019, Hewlett Packard Enterprises (HPE) a lancé HPE GreenLake. Avec cette nouvelle offre, les clients peuvent créer une expérience fluide entre leurs clouds publics et privés, ainsi que gérer et optimiser leur infrastructure IT hybride. HPE avait besoin de fédérer en toute sécurité toutes les identités utilisateurs et authentifier les différents types d'utilisateurs, dont les administrateurs, les équipes de support, les clients et les partenaires — tout cela sur une interface unique.

Grâce à l'intégration B2B d'Okta, HPE peut donner à ses clients professionnels la possibilité de fédérer leurs propres systèmes de gestion des identités et d'isoler leurs propres clients dans un référentiel d'utilisateurs unique. Lorsque les clients se connectent à GreenLake, ils sont dirigés via une intégration Okta spécifique vers leur fournisseur d'identité.

Déployée en deux mois à peine, la plateforme Okta a permis à HPE GreenLake d'offrir une expérience client basée sur une interface conviviale, cohérente avec la marque HPE, avec Okta comme fournisseur en arrière-plan des services de gestion des identités.

PITNEY BOWES

Depuis ses débuts modestes il y a plus d'un siècle en tant qu'entreprise novatrice dans le domaine de l'expédition et du courrier, Pitney Bowes est devenu l'un des plus grands éditeurs de logiciels du monde et prend pied désormais dans l'économie numérique. En 2016, Pitney Bowes a lancé son offre Commerce Cloud pour capturer numériquement toutes les données géographiques et commerciales qu'elle produit, les rendre accessibles via des API à ses collaborateurs, partenaires et clients, et monétiser l'accès à ces API. Il était donc critique de mettre en place une protection adéquate afin de construire un écosystème d'API solide et de collaborer en toute confiance avec des fournisseurs tiers.

L'intégration d'Okta avec Commerce Cloud a amélioré l'accès des clients aux ressources numériques de Pitney Bowes sans nécessiter d'interruptions. Pitney Bowes peut désormais exposer ses fonctionnalités numériques via des API sécurisées, base sur laquelle les développeurs et partenaires peuvent créer des applications.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- **Principales fonctionnalités des solutions CIAM**
- **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
Critères d'une solution CIAM performante

En sachant désormais comment un CIAM avancé 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 CIAM avancée et les critères qui doivent guider votre choix.

Produit

Un CIAM avancé 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 CIAM 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,

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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, intégration avec les API gateways et contrôle des accès aux applications basé sur les rôles.
- *Gestion des utilisateurs :* référentiel 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 en libre-service, la réinitialisation des mots de passe et la récupération des comptes/noms d'utilisateur.
- Interface intuitive d'**administration 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 multifacteur (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 client. 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 de la relation de 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 ont toujours des données à jour sur ces utilisateurs.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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

Plateforme

Comme expliqué dans le chapitre précédent, nous vous recommandons d'adopter une solution CIAM 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 un CIAM prenant en charge un large éventail d'utilisateurs finaux, ce qui inclut les clients, les partenaires et même vos collaborateurs. Un modèle en plateforme constituera une fondation solide qui évoluera en même temps que vos besoins. Par exemple, imaginons que votre entreprise recherche une solution CIAM 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 veut pas dire que vous aurez besoin de deux solutions CIAM distinctes. Un seul CIAM basé sur une plateforme 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 CIAM peut gérer tous ces types d'utilisateurs de façon fluide.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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, il convient de choisir une solution CIAM offrant 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
- Analyse de la 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 sans code.

Enfin, votre CIAM doit assurer une intégration facile via des API, des SDK et des hooks. Avec les inline hooks, vos développeurs peuvent modifier les processus CIAM 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 CIAM 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.

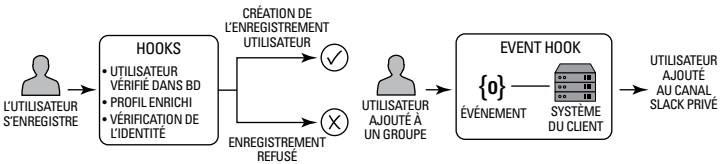

FIGURE 5-1 : Exemple d'inline hook (à gauche) et d'event hook (à droite).

Infrastructure

Un atout majeur d'une solution CIAM 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 des clients explose. En outre, évitez d'avoir à remplacer votre fournisseur CIAM s'il est incapable de tenir le rythme de votre croissance. Recherchez une solution CIAM 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 CIAM 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 :** recherchez un partenaire CIAM offrant une stratégie de sécurité de bout en bout prévoyant différents contrôles :
  - *Sécurité physique et de l'infrastructure :* la sécurité et la disponibilité doivent être intégrées à tous les niveaux : locaux, ordinateurs, réseaux et espaces de stockage.
  - *Personnel sensibilisé à la sécurité :* le fournisseur doit entretenir une culture de la sécurité qui part de la direction et s'étend à toute l'entreprise.
  - *Sécurité du cycle de vie de développement :* des points de contrôle stricts de la sécurité doivent jalonner chaque étape du cycle de vie de développement — de la conception au déploiement en passant par le codage et les tests.
  - *Sécurité des données des clients :* les données de vos clients doivent être protégées en transit et au repos grâce à une technologie de chiffrement sophistiquée, qui répond aux normes les plus sévères, par exemple la NIST (National Institute of Standards and Technology) SP 800-53 et l'ISO (International Organization for Standardization) 27001.
  - *Tests de sécurité et d'intrusion :* votre partenaire doit traquer régulièrement les bugs dans ses logiciels au moyen de tests internes, d'audits de sécurité tiers, d'un programme de Bug Bounty (chasse aux bugs) public, du signalement des bugs par les clients et de tests d'intrusion menés par les clients.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

RAPPEL

Votre solution CIAM a un impact direct sur l'expérience client et sur votre entreprise dans son ensemble. Ce n'est pas votre fournisseur CIAM 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 de confiance et expérimenté, dont la solution CIAM est hautement évolutive, fiable et sécurisée.

Leader du marché

Enfin, lorsque vous évaluez les différentes solutions CIAM avancées disponibles, menez les vérifications nécessaires. La gestion des identités et des accès 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 (Service Organization Control) type I et type II*
  - *Certification STAR (Security, Trust & Assurance Registry) de la CSA (Cloud Security Alliance) niveau 2*
  - *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 de produits, un rôle moteur dans le secteur et une participation à des communautés de développeurs et à des groupes pour l'établissement de normes.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Cartographie du parcours de maturité CIAM
- Les bases pour démarrer
- Automatisation des opérations pour assurer la croissance et l'évolutivité
- Optimisation des expériences clients sans compromettre la sécurité
- Viser l'excellence

Chapitre 6
Exprimer tout le potentiel du CIAM en accord avec vos besoins métier

Le chapitre 5 décrit les critères à prendre en compte dans le choix d'une solution CIAM 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 dans la gestion des identités et des accès clients, ou CIAM.

Le parcours de maturité CIAM

Quel que soit le stade auquel votre entreprise est arrivée dans le parcours de maturité CIAM, 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).

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

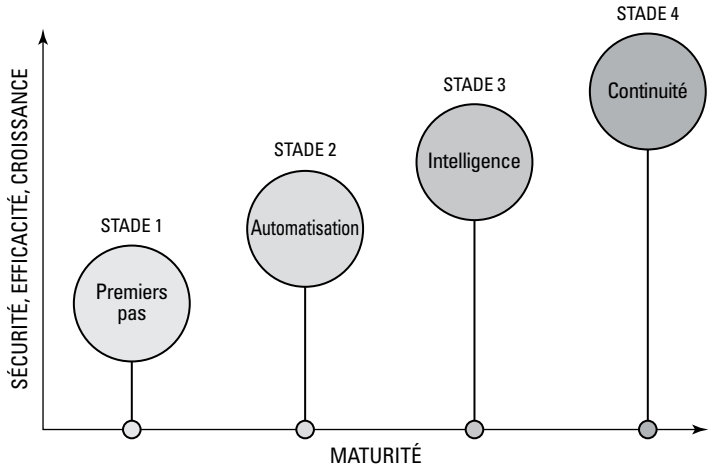

FIGURE 6-1 : Où se trouve votre entreprise sur la courbe de maturité CIAM ?

À chaque stade du parcours de maturité CIAM, 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 au tout 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 :

- Mettre rapidement sur le marché 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 CIAM, où vous devez décider si vous allez utiliser votre temps limité et vos précieuses ressources pour créer votre propre CIAM 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 fonctionnalités CIAM principales 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.

RAPPEL

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 CIAM 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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.

Du point de vue du CIAM, comme les fonctionnalités de gestion des identités sont importantes pour vos clients, vous pouvez envisager de les développer en interne. Toutefois, les objectifs prioritaires à cette étape sont 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 CIAM 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 pourra 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 utilisateurs.
- 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 renforcé 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 de gestion des identités de vos parties prenantes internes (par exemple, les équipes produit, ingénierie et marketing) qui tentent d'offrir une expérience utilisateur fluide et sécurisée à grande échelle.

Une solution CIAM avancée vous aidera de diverses façons à trouver un équilibre entre ces exigences 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 utilisateur 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 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 CIAM 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Continuité : devenir un leader et une référence du secteur

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

RAPPEL

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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- **Des expériences qui susciteront l'engagement de vos clients**
- **Une sécurité renforcée pour gagner la confiance des clients**
- **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 du CIAM

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

Des clients plus engagés

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 du CIAM 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 optimale est donc crucial pour établir des relations positives avec eux.

CONSEIL

Un CIAM avancé conçu pour rester pertinent 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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 maternelle, 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 inoubliable 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.

Une sécurité plus efficace

Afin d'établir des relations de confiance entre vos clients et votre marque, une solution CIAM 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.

Cependant, 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 vraiment 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 CIAM avancés, 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 maintenant et à l'avenir, et susciter 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

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

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) dans certains cas, notamment lorsque 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 devraient exiger un niveau de sécurité plus élevé que les applications 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 le CIAM 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.

Protection de 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 des clients, 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Du point de vue du CIAM, 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 CIAM ou via des intégrations à des solutions de fournisseurs tiers spécialisées 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 d'aujourd'hui et de demain, adoptez une solution CIAM avancée qui gérera à votre place les données à caractère personnel de vos clients en matière de préférences, de confidentialité et de conformité.

Gestion de la complexité

La complexité caractérise la vie des entreprises d'aujourd'hui : 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 CIAM 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, un CIAM 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Checklist pratique pour l'implémentation d'un CIAM
- Identification initiale des exigences techniques et métier
- Choix d'une solution CIAM adaptée à votre entreprise
- CIAM et innovation continue
- Avantage concurrentiel d'une expérience client d'exception

Chapitre 8
Dix considérations liées au CIAM

Ces dix considérations vous aideront à choisir et à implémenter la solution CIAM 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 ?

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **Établissez vos objectifs métier.** Quels sont vos objectifs commerciaux ? L'expansion internationale, le lancement d'un nouveau produit ? Quels sont vos délais ?
- **Listez et analysez vos besoins en matière de CIAM.** Classez vos exigences (métier, expérience utilisateur, sécurité) par ordre de priorité, depuis les « nécessités absolues » jusqu'aux « facultatives ». Faites-les coïncider avec vos besoins internes et déterminez comment trouver le meilleur compromis.
- **Estimez le coût d'opportunité du développement d'un CIAM par rapport à son achat.** Le développement et la maintenance de votre propre CIAM représentent un processus à la fois difficile et coûteux, qui peut vous détourner de vos activités stratégiques. Pour appréhender tout ce qu'implique la création d'un CIAM maison, reportez-vous au chapitre 3.
- **Confiez votre CIAM à un expert externe (pour obtenir une solution de qualité).** Maintenant que vous savez ce que vous recherchez et avez déterminé votre coût d'opportunité, identifiez l'expert CIAM qui convient. Recherchez un partenaire de confiance ayant une solide expérience en la matière, qui sera capable de répondre à vos besoins actuels et futurs.
- **Déployez des expériences clients fluides.** Une fois que vous avez choisi votre solution CIAM avancée, vous pouvez la déployer rapidement et largement 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 CIAM.** Une solution CIAM 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 CIAM, reportez-vous au chapitre 6.
- **Concentrez-vous sur votre avantage concurrentiel.** Un CIAM avancé 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.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Ltd. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

CIAM:
Le guide pour les nuls qui répond à vos questions.

auth0

auth0.com/fr/ciam

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 une solution de gestion des identités et des accès clients, ou CIAM (Customer Identity & Access Management). Le CIAM offre une couche d'identités numérique qui peut s'intégrer aux applications, sites web et portails accessibles au grand public. Dans ce livre, vous découvrirez comment une solution CIAM peut vous aider à offrir des expériences sécurisées et fluides à vos clients et partenaires.

À l'intérieur…

- Les concepts fondamentaux du CIAM
- Pourquoi le CIAM est plus important que jamais
- Pourquoi il n'est pas recommandé de développer un CIAM maison
- Qu'est-ce qu'une solution CIAM avancée ?
- Critères d'une solution CIAM performante
- Les atouts d'une solution CIAM adaptée à vos besoins métier
- L'avenir du CIAM

auth0

Lawrence C. Miller est expert 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.

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-119-86657-2
Revente interdite

pour les nuls®

WILEY END USER LICENSE AGREEMENT

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