okta

Transformer l'expérience client à l'aide d'une solution avancée de gestion des identités et des accès clients (CIAM)

Okta France
Paris

paris@okta.com
01 85 64 08 80

« L'éventail toujours plus large de canaux, de terminaux, de plateformes et de points de contact accentue le besoin de solutions CIAM. »

Un paysage en mutation constante

Aujourd'hui, pratiquement toutes les entreprises intègrent les technologies dans leurs opérations métier dès lors qu'elles mettent en œuvre la transformation numérique de leurs expériences clients. Face à la multiplication des terminaux, à l'évolution rapide des exigences des clients et à leurs attentes élevées en matière de sécurité et de confidentialité, les entreprises en quête de réussite doivent veiller à ce que leurs clients puissent utiliser leurs applications mobiles ou leurs services de manière sécurisée, à tout moment et depuis n'importe quel terminal.

C'est là qu'intervient la gestion des identités et des accès clients (CIAM, Customer Identity and Access Management). Le CIAM permet de créer et de déployer rapidement des expériences clients évoluées et fluides, tout en répondant au besoin d'une gestion des identités, d'une sécurité et d'une évolutivité pérennes. Le CIAM constitue une technologie essentielle pour respecter les exigences toujours plus complexes des clients et permet aux entreprises de proposer des expériences numérisées sécurisées et fluides.

L'éventail toujours plus large de canaux, terminaux, plateformes et points de contact accentue le besoin d'une gestion des identités et des accès clients performante. Mais une solution CIAM ne se limite pas à autoriser l'accès aux ressources appropriées à la bonne personne, au bon moment.

Les solutions CIAM étaient traditionnellement utilisées pour les cas d'usage orientés consommateurs (B2C). Toutefois, une entreprise peut également compter parmi ses clients une autre société (B2B). Les attentes des clients vis-à-vis des entreprises avec lesquelles ils traitent étant plus élevées, les exigences peuvent s'étendre à diverses cibles et cas d'usage. Ainsi, les entreprises qui développent des applications mobiles destinées à leurs clients seront peut-être amenées à afficher des données sur le stock, généralement extraites d'un système ERP connecté à une solution IAM (Identity and Access Management) destinée aux collaborateurs. De même, les collaborateurs devront sans doute accéder aux données d'expériences clients pour résoudre des problèmes rencontrés par les clients. Il ne s'agit là que de quelques exemples : des intégrations plus variées sont opérées entre les applications et les types d'utilisateurs au quotidien.

Résultat : les solutions CIAM proposées par les éditeurs s'imposent plus que jamais comme des outils incontournables pour les entreprises. Plus de 69 % des participants à une étude réalisée par Gartner sur la gestion des identités et des accès utilisent, ou prévoient d'utiliser, diverses technologies IAM pour des clients B2C d'ici la fin 2018*. Gartner recommande aux entreprises de « concevoir et de gérer [leur] système CIAM comme une plateforme stratégique* ».

Tendances majeures en matière de conception de solutions CIAM

Lorsque les entreprises envisagent l'adoption d'une solution CIAM et se chargent de sa conception, elles doivent tenir compte des changements survenus dans le domaine des identités clients. Voici quatre tendances majeures qui doivent inspirer les entreprises dans leur conception d'une solution CIAM répondant à leurs besoins actuels et à venir :

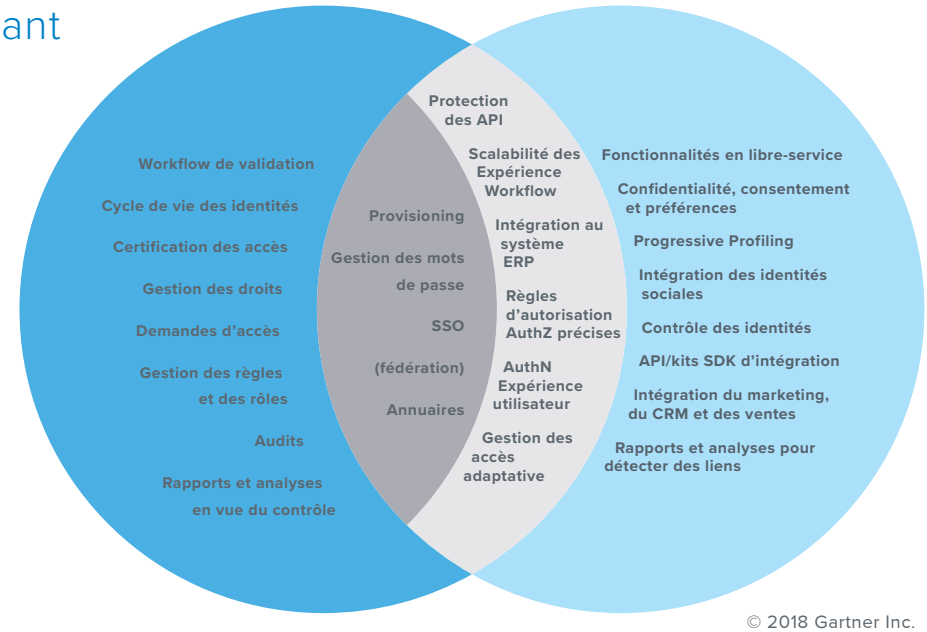
Chevauchement croissant des fonctionnalités CIAM et IAM

Une solution CIAM cible généralement les consommateurs, mais la complexification de l'expérience client, les cibles supplémentaires à prendre en compte ainsi que les chevauchements entre les cas d'usage nécessitent des fonctionnalités IAM plus classiques. Les solutions IAM traditionnelles permettent depuis longtemps de contrôler avec précision les autorisations d'accès et les mesures de sécurité, ce qu'imposent de plus en plus les cas d'usage CIAM. Comme le montre la figure ci-dessous, nous allons assister à une augmentation constante du nombre de fonctionnalités IAM à exploiter, tant pour le déploiement d'une solution IAM orientée consommateurs, que pour celui d'une solution IAM axée collaborateurs.

Les zones de chevauchement habituelles (apparaissant dans la zone gris foncé et publiées dans le cadre d'une étude réalisée fin 2016) comprennent uniquement quelques fonctionnalités essentielles, telles la gestion des mots de passe et l'authentification unique. Toutefois, le chevauchement fonctionnel entre l'IAM et le CIAM s'étend rapidement avec l'ajout de nouvelles fonctionnalités (apparaissant dans la zone gris clair et ajoutées seulement 1,5 an après).

L'une des fonctionnalités communes est la protection des API, notamment contre les attaques malveillantes et les menaces, à l'image de celles prenant en charge les applications mobiles. La gestion des accès adaptative en est un autre exemple. Cette fonctionnalité repose sur des politiques d'accès et d'authentification intelligentes, basées sur le contexte de la connexion (notamment l'emplacement, ou le terminal et le réseau utilisés). La gestion des accès adaptative

Chevauchement croissant des fonctionnalités CIAM et IAM



Gartner, figure 3, Les fonctionnalités communes au **CIAM et à l'IAM ciblant les collaborateurs sont toujours plus nombreuses**, *Top 5 Trends in CIAM Solution Design,*
5 March 2018

Source: Gartner (March 2018)

peut limiter les risques liés à l'authentification, sans pour autant créer davantage de points de friction pour l'ensemble des utilisateurs d'une entreprise (consommateurs, collaborateurs, partenaires et autres utilisateurs). Parallèlement, un contrôle très précis des autorisations, traditionnellement associé aux collaborateurs et aux partenaires commerciaux accédant à des données sensibles, s'applique désormais aux clients qui bénéficient d'un accès aux seules informations dont ils ont besoin.

D'après l'étude, le chevauchement entre le CIAM et d'autres déploiements de solutions IAM est de plus en plus important. Les implémentations répondant aux besoins de plusieurs types d'utilisateurs se généralisent (par exemple, B2C comme B2B, ou IoT comme B2C, sur la même plateforme CIAM*). Les cas d'usage du CIAM imposent de plus en plus le respect d'exigences importantes en matière d'IAM axé collaborateurs, comme le cycle de vie des identités, dans le but de contrer les attaques malveillantes. Les audits, rapports et analyses en vue du contrôle sont également essentiels pour associer étroitement les déploiements CIAM avec la sécurité d'une entreprise et ses processus orientés DevOps. D'autre part, les principales exigences du CIAM liées aux kits SDK ou API d'intégration et aux fonctionnalités en libre-service sont désormais mises en œuvre dans les solutions IAM axées collaborateurs pour un développement applicatif évolué. Sans compter que ces collaborateurs ont eux-mêmes des attentes en matière d'expériences clients. Cette implémentation unique peut optimiser l'efficacité opérationnelle et devrait également s'adapter aux besoins en constante évolution des entreprises et de leurs utilisateurs.

Expériences omnicanales fluides et cohérentes, facilitées par l'authentification unique (SSO)

Les clients utilisent un grand nombre de terminaux, et ce nombre ne cesse de croître. Les systèmes d'identification biométrique en tant que second facteur d'authentification, ainsi que l'accès sans mot de passe, sont de plus en plus plébiscités par les clients.

C'est la raison pour laquelle les entreprises devraient s'efforcer de réduire les points de friction superflus, qui augmentent l'attrition client. La gestion des identités clients peut donc représenter un défi de taille : les entreprises doivent prendre en charge l'ensemble de ces canaux, mais également veiller à ce que l'expérience utilisateur soit optimisée pour chacun d'entre eux, tout en assurant sa cohérence d'un canal à l'autre.

Pour y parvenir, Gartner recommande de proposer

« une procédure de connexion unifiée (SSO) sur l'ensemble des propriétés numériques, si celle-ci n'est pas déjà mise en place par l'entreprise ». Une connexion unique permettant d'accéder à l'ensemble des systèmes orientés grand public de l'entreprise limite les points de friction pour le consommateur et fournit une source unique d'informations de premier niveau et faisant autorité*.

Amélioration de l'assistance aux développeurs

Dans un monde où les technologies font partie intégrante des activités des entreprises, les systèmes CIAM doivent offrir une plateforme permettant une évolution permanente, et ces systèmes deviennent des plateformes de développeurs qui gagnent en flexibilité. Les développeurs jouent un rôle clé dans la conception d'expériences clients élaborées. Ils ont besoin d'une solution CIAM agile qui écourte les délais de mise sur le marché pour s'adapter à l'évolution rapide des besoins des clients. En outre, une solution CIAM doit aider les développeurs à offrir une couche d'identités pour des expériences clients sécurisées. Ainsi, ils n'ont pas à réinventer la roue pour ce qui est de la gestion des authentifications, autorisations et utilisateurs, ce qui leur permet de se concentrer sur les fonctionnalités différenciant leur application des autres.

Parmi les nombreux composants d'une solution CIAM, les entreprises doivent privilégier des fonctionnalités davantage adaptées aux développeurs, telles que :

- **des API bien documentées avec un échantillon de code ;**
- **la prise en charge des langues et du framework (SDK) ;**
- **une documentation complète ;**
- **une interface utilisateur et des workflows personnalisables ;**
- **l'intégration possible avec des gateways d'API ;**
- **la prise en charge du traitement orienté événements.**

Gartner suggère d'opter pour des offres CIAM comprenant des fonctionnalités qui facilitent encore la tâche des développeurs afin de s'adapter constamment à l'évolution des besoins clients et métier*. Une solution CIAM doit être orientée développeurs et suffisamment agile pour prendre en charge de nouveaux protocoles, services, architectures et autres améliorations.

Renforcement de la sécurité et de la conformité

La sécurité est primordiale : les données clients peuvent être compromises en une seconde à peine. Et lorsqu'une violation de sécurité de produit, elle peut avoir de lourdes conséquences sur la viabilité d'une entreprise et la façon dont les clients la perçoivent.

Cet état de fait met en lumière le besoin de fonctionnalités et de solutions de nouvelle génération en matière de sécurité.

Selon Gartner, « une architecture de sécurité est indispensable à toute initiative dans le domaine du CIAM* ». Les accès clients doivent être protégés à l'aide de méthodes d'authentification adaptatives, selon une approche contextualisée permettant de vérifier l'identité d'un client. Les entreprises doivent réfléchir aux méthodes à employer pour sécuriser les interactions avec les clients, tout en poursuivant leurs optimisations en vue de l'ergonomie et d'une expérience d'authentification fluide. La gestion des accès adaptative doit tenir compte d'éléments d'identification dynamiques (comme l'emplacement du client, son terminal, son adresse IP et d'autres données collectées par le fournisseur). Par exemple, les clients qui utilisent un nouveau terminal pour se connecter à une application sensible seront invités à procéder à une authentification multifacteur (MFA, Multi-Factor Authentication). Par contre, les clients qui se connectent à l'aide d'un mobile déjà enregistré peuvent s'authentifier sans mot de passe, ce qui se traduit par un renforcement de la sécurité et une optimisation de l'ergonomie.

Comme le précise l'étude, « la plupart des initiatives orientées consommateurs comptant parmi les plus complexes, telles que la création d'une application mobile personnalisée ou d'une nouvelle application basée sur le navigateur, nécessitent de développer de nouvelles API auxquels les consommateurs accèdent sur le Web. Ces API externes doivent être protégées en associant des mesures de sécurité et d'autres relatives à l'IAM. Pour toute API consommée en externe (et pour de nombreuses API internes), une gateway d'API, généralement intégrée à une solution plus globale de gestion du cycle de vie des API, doit être comprise dans l'infrastructure de protection des API.

S'agissant des cas d'usage du CIAM, le système CIAM est un fournisseur d'identité qui se connecte à la gateway d'API à l'aide d'OAuth et/ou d'OpenID Connect. Selon le cas, vous pouvez également avoir besoin d'une ou plusieurs des nouvelles extensions de la norme OAuth* ».

Outre la sécurité, les entreprises doivent également anticiper la mise en conformité. Les mesures visant à protéger les données clients sont toujours plus rigoureuses, comme en témoigne la portée mondiale du Règlement général sur la protection des données (RGPD) de l'Union européenne, la nouvelle loi californienne sur la confidentialité des données et les normes propres à certains secteurs d'activité, comme l'authentification multifacteur pour les applications financières à New York. Une solution CIAM permet de garantir un parcours client fluide dans toute juridiction grâce à une approche automatisée en matière de respect des principales normes.

Okta Identity Cloud : une solution CIAM avancée

Une solution évoluée de gestion des identités et des accès clients doit respecter les normes de sécurité et de conformité actuelles, mais aussi tenir compte des contraintes qu'implique la création d'expériences clients fluides et à la pointe de la technologie. C'est précisément ce que fait Okta Identity Cloud en proposant l'une des solutions CIAM les plus sécurisées et fiables du secteur pour la protection des données clients, tout en mettant à disposition des développeurs une série d'outils sophistiqués pour assurer une agilité à long terme.

Okta est né et a grandi dans le cloud. La solution Okta Identity Cloud propose un service unique, complet et intégré, pour tout type d'utilisateur. Avec des fonctionnalités adaptées à des cas d'usage communs à l'IAM et au CIAM, Okta Identity Cloud fournit un système centralisé de contrôle d'accès à chaque expérience, et permet aux équipes IT qui gèrent les accès des utilisateurs et aux développeurs qui créent des expériences clients de travailler plus efficacement. La solution évolue pour répondre efficacement aux exigences de toute entreprise et, ce faisant, elle permet à des millions d'utilisateurs d'accéder en toute sécurité aux expériences dont ils ont besoin. Les entreprises peuvent choisir d'utiliser les fonctionnalités prêtes à l'emploi d'Okta ou de tirer parti des API et toolkits d'Okta pour créer des expériences clients sur mesure.

Okta Identity Cloud est en phase avec toutes les tendances majeures en matière de conception de solutions CIAM, grâce à un certain nombre de produits et fonctionnalités :

Authentification unique (SSO)

Okta Identity Cloud propose des fonctionnalités d'authentification unique (SSO, Single Sign-On), qui permettent d'associer tout groupe de portails et d'applications avec un jeu unique d'identifiants — voire, dans le cas d'une authentification sans mot de passe, aucun identifiant. Un seul clic suffit aux utilisateurs pour se connecter à toutes leurs applications.

Authentification multifacteur adaptative

La solution d'authentification multifacteur adaptative (MFA, Multi-Factor Authentication) d'Okta associe un grand nombre de seconds facteurs avec un cadre de règles strict, permettant ainsi de prévenir les usurpation d'identité grâce à une couche supplémentaire d'authentification. Cette fonctionnalité permet aux entreprises de définir des règles pour demander une authentification multifacteur en fonction du profil de l'utilisateur, de l'application utilisée et du contexte d'authentification. Grâce à la prise en charge d'une série de facteurs de vérification tels que le SMS, les envois de notifications avec Okta Verify et les données biométriques, la solution multifacteur adaptative d'Okta permet d'offrir le niveau de sécurité correspondant aux différents besoins des utilisateurs.

Annuaire universel

Okta Universal Directory fournit aux entreprises une solution de gestion centralisée des utilisateurs, des applications, des terminaux et des API. Cet annuaire universel peut stocker un nombre illimité d'attributs clients, dont leurs préférences en matière de consentement et de confidentialité de leurs données. En outre, il peut être synchronisé avec n'importe quelle application ou n'importe quel annuaire pour offrir une vue à 360 degrés d'un client. Les entreprises ont ainsi la possibilité de mettre en place un référentiel centralisant les informations d'identité des utilisateurs, à partir duquel elles pourront créer une expérience cohérente et personnalisée dans l'ensemble de leurs applications.

Gestion des accès aux API

De plus en plus d'applications personnalisées sont développées avec un backend d'API. Les fonctionnalités du composant API Access Management d'Okta sont adaptées à des applications mobiles et web évoluées, avec une prise en charge du protocole OAuth 2.0. Ces outils permettent de gagner deux semaines par développeur et par an, ainsi que de protéger un nombre illimité de ressources API derrière n'importe quelle gateway dédiée.

API et outils développeurs

Les API et outils développeursd'Okta offrent un accès par programmation à Okta Identity Cloud. Cet accès permet ainsi aux développeurs d'ajouter des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs à leurs applications en quelques minutes. Okta met à disposition des développeurs des toolkits (SDK) dans chaque grand environnement de programmation, assortis d'une série de documents et d'assistants de démarrage rapide pour optimiser leur productivité. Inscrivez-vous dès aujourd'hui pour créer un compte développeur Okta gratuitement et vous lancer.

Analyses de sécurité et conformité

Okta adopte une approche complète de la sécurité par le biais de son infrastructure et de ses processus contrôlés et sécuriséshttps://www.okta.com/security/, qui comprennent les stratégies et opérations liées au personnel, au cycle de développement et aux data centers. De plus, Okta améliore la visibilité globale et le temps de réaction grâce à des rapports en temps réel, qui peuvent également être intégrés dans une solution d'analyse de sécurité.

Okta Integration Network

Le vaste réseau d'intégrations d'Okta permet aux développeurs de mettre plus rapidement sur le marché de nouvelles applications, tout en protégeant les clients et en leur proposant une expérience utilisateur fluide, au moyen d'intégrations telles que des gateways d'API et un contrôle des identités.

Okta Identity Cloud propose une multitude de fonctionnalités CIAM. C'est la raison pour laquelle Okta est la solution CIAM leader conçue pour protéger les comptes clients, interagir avec davantage d'utilisateurs et doper le chiffre d'affaires des entreprises.

LE SAVIEZ-VOUS ?

Okta a été désigné comme leader dans l'étude « IdaaS and Access Management Magic Quadrant » de Gartner ces cinq dernières années**.

PRÊT À VOUS LANCER ?
Contactez-nous

*Gartner, « Top 5 Trends in CIAM Solution Design », 5 mars 2018

**Garner Inc., « Magic Quadrant for Access Management, Worldwide », Gregg Kreizman, 18 juin 2018

Le cabinet Gartner ne soutient aucun fournisseur, produit ou service décrit dans ses études, pas plus qu'il ne conseille aux utilisateurs potentiels de choisir exclusivement les fournisseurs ayant obtenu les meilleures notes ou une reconnaissance particulière. Les études Gartner consignent les avis émis par le cabinet Gartner et ne doivent pas être considérées comme des énoncés de faits. Gartner décline toute garantie, expresse ou implicite, concernant cette étude, et notamment toute garantie de qualité marchande ou d'adéquation à un usage particulier.