Livre blanc

Le CIAM, pour un juste équilibre entre sécurité et expérience client

La sécurité est une cible mouvante. Une solution CIAM robuste peut vous aider à trouver le juste équilibre entre vos besoins et ceux de vos clients.

Avez-vous fermé à clé la porte d'entrée ?

Vous ne savez plus où donner de la tête : un café à la main, vous devez gérer les enfants, les sacs de course et le chat qui tente de se faufiler. C'est dans ce genre de situation que l'on peut oublier les gestes essentiels, comme fermer une porte à clé.

Au travail aussi, c'est une course de vitesse : les derniers résultats de l'enquête clients viennent de tomber, votre chef de projet veut organiser une réunion à la pause déjeuner et vous allez être en retard à votre réunion d'équipe hebdomadaire. Ajoutez à cela l'accélération de la transition digitale dans tous les secteurs et les effets durables de la pandémie, et vous allez devoir travailler à une vitesse supersonique.

Selon Twilio, entre les efforts déjà consentis et l'accélération provoquée par la pandémie, les entreprises ont dû avancer leur transformation IT de 6 ans en moyenne, voire près de 10 ans dans certains secteurs. 97 % des décideurs ayant participé à ce sondage estiment que la pandémie est responsable de cette accélération. Pour gérer l'adoption de l'omnicanal au plus vite pour vos clients, votre prochaine version doit inclure un système unifié de gestion des utilisateurs.

Une solution de gestion des identités et des accès clients (CIAM) vous permet d'intégrer, d'organiser et de gérer les comptes et données clients depuis un emplacement centralisé.

La page de connexion est la porte d'entrée de votre entreprise pour vos clients. C'est le premier élément visible pour l'utilisateur : l'expérience du flux de connexion doit donc être irréprochable. C'est également la première cible de nombreux cybercriminels à l'affût d'une vulnérabilité à exploiter pour faire main basse sur vos données. Elle doit donc être impérativement sécurisée. Reste à déterminer le niveau de sécurité à y appliquer… Allez-vous laisser des ouvertures qui permettront à n'importe qui d'entrer ? Ou allez-vous ajouter un gros verrou et une chaîne pour obliger les utilisateurs à frapper et à attendre qu'on vienne leur ouvrir ? Si le niveau de sécurité est trop faible, tout le monde pourra entrer. S'il est trop fort, les clients seront vite découragés. Il s'agit de trouver un équilibre entre sécurité et expérience client.

Une solution de gestion des identités et des accès clients (CIAM) vous permet d'intégrer, d'organiser et de gérer les comptes et données clients depuis un emplacement centralisé. Un outil CIAM robuste vous permettra également de définir les mesures de sécurité appropriées pour préserver la sécurité des données clients tout en limitant le nombre de points de friction de l'expérience utilisateur.

Si l'accès est trop compliqué, vous perdrez des conversions — qu'il s'agisse d'un nouvel utilisateur qui abandonnera au bout du troisième CAPTCHA, ou d'un client fidèle rebuté par une réinitialisation des mots de passe trop complexe. Ce sont de tels points de fiction qui poussent parfois les utilisateurs à abandonner la procédure et à tourner le dos à votre entreprise. Ils entraîneront leurs amis sur la même voie, ce qui aura des conséquences désastreuses à long terme pour votre marque.

Porte d'entrée numérique de votre entreprise, la solution CIAM occupe une position unique au carrefour de la sécurité, de la confidentialité et de la fluidité. Trouver le bon dosage entre ces trois exigences de base pour votre produit et vos clients peut être complexe. Si vous affectez des ressources de développement à la création de votre propre solution, vos développeurs et autres ressources ne pourront plus se consacrer au produit. Votre équipe de développement excelle dans son domaine. Elle mobilise tous ses talents pour développer le meilleur produit possible. Pourquoi ne pas apporter le même soin à l'expérience de connexion et à la protection des données de vos clients et confier la gestion des identités à des spécialistes ?

En optant pour une solution SaaS dédiée pour la gestion des identités, vous permettrez à vos développeurs de mettre tout leur talent au service du produit, et vous serez assuré que tout sera mis en œuvre pour protéger les informations de vos clients, ce qui contribuera grandement à établir la confiance dans votre marque. Selon le rapport Trust Barometer 2020 d'Edelman, la confiance et la réputation de la marque figurent ensemble en deuxième position de la liste des facteurs déclencheurs des décisions d'achat, derrière le prix.

Optimisation de la sécurité, de la confidentialité et de la fluidité grâce au CIAM

Parallèlement à l'accélération de la transition digitale dans tous les secteurs, une augmentation du nombre de cyberattaques ciblant le périmètre accessible au public a été observée. La protection de l'intégrité et de la réputation de la marque est devenue une priorité pour la plupart des dirigeants d'entreprise. Le verrouillage du périmètre exposé aux clients devient donc indispensable. Les brèches de données peuvent être très préjudiciables, non seulement pour la réputation de votre marque, mais également pour votre chiffre d'affaires. Leurs conséquences peuvent se faire sentir des années après l'incident. Tout mettre en œuvre pour prévenir de telles attaques est donc une stratégie qui semble aller de soi.

Pour la plupart des entreprises, le succès est étroitement lié au nombre de conversions. Les points de friction pouvant nuire à ces conversions, il convient donc d'assurer la fluidité de la page de connexion.
Grâce au CIAM, vous avez la capacité de contrôler le flux de l'expérience de connexion de vos clients, ainsi que les données nécessaires pour faire évoluer cette expérience en fonction des besoins. En trouvant le juste équilibre entre sécurité, confidentialité et expérience client tant pour votre entreprise que pour vos clients, vous atteindrez le niveau de sécurité nécessaire et l'expérience fluide exigée.

Les avantages du CIAM ne se limitent cependant pas à fluidité de la page de connexion. Une solution CIAM robuste combine une expérience utilisateur optimale avec une protection contre les cyberattaques, la confidentialité des données utilisateurs et des contrôles intuitifs de gestion des comptes utilisateurs.

Le CIAM vous protège contre les vecteurs d'attaque courants en renforçant vos défenses au périmètre

Prenons un cas d'utilisation théorique : l'élargissement de la présence web de votre entreprise. Vous venez de faire l'acquisition d'une startup d'e-commerce en même temps que vous achevez le développement d'un portail réservé aux membres, dédié à des promotions ponctuelles, en complément de vos applications et magasins web actuels. Votre équipe est chargée de rassembler tous ces éléments en une interface unifiée, via une nouvelle application web. C'est le moment idéal pour intégrer une solution CIAM extensible et évolutive qui permettra à vos clients d'accéder à tous les sites au moyen d'un seul jeu d'identifiants, ce qui réduira votre surface d'attaque.

De plus, les solutions CIAM qui offrent des fonctionnalités telles que la détection des bots et le support à la correction, l'intégration avec le MFA et le log streaming, renforcent encore vos défenses.
Dans les architectures distribuées actuelles, l'identité est le périmètre.

L'extensibilité, l'évolutivité et l'intégration de partenaires sont des fonctionnalités à exiger d'une solution CIAM pour permettre à votre entreprise de se développer tout en assurant la protection de votre périmètre et de vos données.

> Par l'application de règles minimales en matière de mots de passe (y compris des règles de réutilisation), l'optimisation du flux de réinitialisation des mots de passe et l'intégration de l'authentification multifacteur (MFA), les solutions CIAM resserrent votre périmètre des identités.

Un grand nombre d'attaques fonctionnent grâce au phénomène de réutilisation des mots de passe. Une récente enquête réalisée par LogMeIn, concepteur du gestionnaire de mots de passe Lastpass, montre que même si 91 % des utilisateurs sont conscients que réutiliser des mots de passe constitue un risque pour la sécurité, 66 % recourent à cette pratique. Une solution CIAM peut vous aider à faire respecter de bonnes pratiques dans ce domaine. Par l'application de règles minimales en matière de mots de passe (y compris des règles de réutilisation), l'optimisation du flux de réinitialisation des mots de passe et l'intégration de l'authentification multifacteur (MFA), les solutions CIAM resserrent votre périmètre des identités.

Les données utilisateurs consolidées sont plus faciles à protéger

Le concept de « source fiable unique » (SSoT, Single Source of Truth) est un cadrage de gestion des données selon lequel il est préférable pour une entreprise de disposer d'un emplacement centralisé pour le stockage de toutes les données pertinentes, plutôt que de plusieurs sites fragmentés. Le CIAM étend ce concept à vos données utilisateurs en regroupant toutes les informations de comptes en un seul emplacement. Quel que soit le nombre de plateformes utilisées pour le stockage de vos applications, votre solution CIAM sera en mesure de gérer tous les comptes utilisateurs et de diriger toutes les données entrantes vers la même source fiable unique des identités.

Il vous sera alors bien plus facile de protéger ces données stockées à un seul endroit. La gestion centralisée des comptes utilisateurs est également indispensable pour rester en conformité avec les principales réglementations en matière de confidentialité des données. Le règlement RGPD et la loi CCPA obligent par exemple les entreprises à fournir sur demande de l'utilisateur une copie de ses données, ainsi que des informations sur le mode d'utilisation de celles-ci. Ces règles s'appliquant également aux systèmes et données des partenaires, le CIAM vous offre l'accès dont vous avez besoin pour préserver votre conformité tout en satisfaisant vos clients.

Votre source fiable unique des identités permet également d'améliorer l'expérience utilisateur. Grâce à l'authentification unique (SSO) qui récupère les informations pertinentes depuis votre source fiable unique, vos utilisateurs n'auront à mémoriser qu'un seul jeu d'identifiants. Si vos clients sont satisfaits, ils resteront fidèles à votre application et vous réduirez le nombre de comptes orphelins vulnérables aux attaques. Satisfaire toutes les parties prenantes n'est pas une tâche facile. L'utilisation d'un outil CIAM modulaire en mode SaaS peut vous aider à atteindre cet objectif.

L'optimisation des processus facilite la vie des utilisateurs

Lorsqu'un client crée un compte ou se connecte à un compte existant, il vous fait confiance. Il espère également que son parcours sera suffisamment fluide pour ne pas le décourager et l'obliger à abandonner la procédure. Si la procédure que vous avez conçue ne comprend que quelques étapes intuitives lui permettant de s'authentifier et d'utiliser rapidement son nouveau compte, il saura qu'il a eu raison de vous faire confiance.

Une solution CIAM doit être en mesure d'effectuer toutes ces tâches : optimiser la procédure de création de compte pour que les nouveaux utilisateurs se sentent bien accueillis et sachent que les procédures de traitement de leurs données sont sécurisées. Selon PwC, pas moins de 32 % des clients se détournent d'une marque dès la première mauvaise expérience. Oui, vous avez bien lu. Un tiers des personnes interrogées déclarent couper toute relation avec une entreprise après une seule expérience désagréable. Imaginez ce que ces clients mécontents vont dire à leurs amis si cette mauvaise expérience a été leur première rencontre avec votre entreprise ? Comme vous le verrez dans la section suivante, le CIAM permet d'homogénéiser vos procédures et flux de comptes utilisateurs.

Un cycle de vie utilisateurs simplifié est plus facile à sécuriser

La création d'un nouveau compte n'est pas toujours le fait d'un nouveau client. Il peut en effet s'agir d'un client existant qui a oublié son mot de passe et a été découragé par un flux de réinitialisation des mots de passe

trop complexe. Résultat : vous allez être amené à gérer un compte double sans le savoir. Tout au long du cycle de vie utilisateur, une solution CIAM entièrement intégrée offre des avantages en matière de sécurité.

Création de compte

Afin d'éviter les abandons de compte, il est indispensable que la procédure de création soit aussi fluide que possible tout en prévoyant une vérification de l'identité des utilisateurs. C'est ce que permettent les solutions CIAM intégrant le SSO. En autorisant un utilisateur à se connecter à partir d'un compte de réseau social existant, vous avez la garantie que son identité a déjà été vérifiée et que l'utilisateur pourra créer son nouveau compte en quelques secondes. Cette procédure intuitive réduit la réutilisation des mots de passe, limite le risque de compromission des comptes et améliore la protection des données.

Gestion des comptes

En matière de maintenance des comptes utilisateurs, l'automatisation est votre alliée. Votre solution CIAM doit vous permettre d'automatiser le flux de réinitialisation des mots de passe afin de garantir la fluidité de cette procédure très courante. En complément, une plateforme complète de gestion des comptes offre des options MFA qui permettent de contrôler rigoureusement l'identité de la personne se connectant. La fédération des identifiants permet d'identifier un compte double créé accidentellement par un utilisateur et de le combiner à l'autre compte dans votre source fiable unique des identités. La sécurité renforcée fournie par le MFA et l'élimination des comptes doubles ou orphelins permettent de limiter les risques de brèche.

Fin de vie d'un compte

Qu'advient-il d'un compte oublié par son utilisateur, transféré vers un autre produit ou totalement abandonné ? Dans la plupart des cas, il ne se passe rien. Si les bonnes pratiques de gestion des comptes ne sont pas appliquées, votre source fiable unique va être encombrée de comptes abandonnés, inutilisés et redondants. Cela pose non seulement un problème de maintenance, mais également de sécurité. Ces identifiants peuvent être impliqués dans des brèches de données et utilisés pour attaquer vos systèmes. Diverses fonctionnalités automatisées de gestion des comptes permettent de neutraliser ce vecteur d'attaque fréquent — notamment l'envoi d'e-mails à des comptes non utilisés pendant une période prédéterminée, la désactivation automatique de comptes et leur suppression éventuelle.

La compromission d'identifiants expose à divers vecteurs d'attaque

Du fait de mauvaises pratiques liées aux mots de passe, les identifiants utilisateurs volés lors d'une brèche de données peuvent être réutilisés à l'infini pour s'introduire dans de nombreux autres sites. Les cybercriminels n'ont aucun mal à obtenir des noms d'utilisateurs et des mots de passe, même s'ils ne sont pas assez qualifiés pour procéder eux-mêmes à une brèche de données.

Ces pirates sans compétences techniques particulières peuvent acheter une liste d'identifiants sur le Dark Web, puis utiliser des scripts préexistants ou de véritables applications, également disponibles sur le Dark Web, pour lancer une intrusion au moyen du credential stuffing ou de toute autre attaque de type force brute. Vous devez connaître ces vecteurs d'attaque et savoir comment ils sont utilisés pour être en mesure d'intégrer votre solution CIAM le mieux possible dans votre cas d'usage.

Credential stuffing

Les attaques par force brute appelées « credential stuffing » constituent l'un des vecteurs d'attaque les plus courants. Dans ce type d'attaque, un cybercriminel utilise une liste de noms d'utilisateurs et de mots de passe et les applique au flux de connexion de différents sites. Le phénomène répandu de la réutilisation des mots de passe est ce qui fait l'attrait d'un tel vecteur, car il existe de fortes chances que les identifiants qu'ils testent fonctionneront suffisamment souvent pour que le jeu en vaille la chandelle. Ces attaques misent sur la paresse des utilisateurs et la réutilisation de mots de passe de base, faciles à déchiffrer (le mot de passe le plus souvent utilisé actuellement est « 123456 », suivi de près par « password ».)

Compromission de la messagerie d'entreprise (BEC)

La compromission des mots de passe peut servir à mener d'autres attaques. Un cybercriminel peut, par exemple, acheter une liste d'identifiants associés à l'entreprise qu'il souhaite attaquer. En usurpant l'identité de cadres supérieurs au moyen de leurs identifiants réseau dérobés, il peut envoyer des e-mails de phishing ciblés (ou spear phishing) semblant provenir de la personne légitime. Ces attaques, de plus en plus fréquentes du fait de l'utilisation de bots, servent principalement aux attaques de social engineering jouant sur le facteur humain pour parvenir à leurs fins.

Attaques de bots

Certains cybercriminels veulent seulement perturber le fonctionnement des systèmes de l'entreprise qu'ils ciblent. Leur intention n'est pas de voler quoi que ce soit, mais simplement de marquer le coup en paralysant les opérations tandis que l'entreprise ciblée tente de neutraliser l'intrusion et de faire repartir son activité. Les attaques par déni de service distribué (DDoS) en sont un exemple très courant. Le cybercriminel utilise des bots pour submerger un site par un énorme volume de trafic, le rendant inaccessible à des visiteurs légitimes pendant un certain temps. Ces attaques finissent par coûter cher à l'entreprise visée en termes de réputation et de pertes financières liées à l'interruption de l'activité.

Les bots peuvent être également utilisés pour prendre d'assaut le flux de connexion d'un site d'e-commerce afin d'épuiser le stock d'articles très recherchés. Les bots en essaim ont été récemment utilisés lors du lancement par Nvidia d'une nouvelle carte graphique attendue avec impatience par des joueurs du monde entier. Il en a été de même lorsque Microsoft a lancé la X-Box X et Sony la très attendue PlayStation 5. Des sites tels que Walmart et Amazon ont vu leurs capacités de traitement mises à rude épreuve par des centaines de milliers de comptes créés par des bots et utilisés pour acquérir tout le stock disponible afin de faire grimper les prix sur le marché secondaire. Ces attaques provoquent une chute de la disponibilité de biens de premier ordre, empêchent les utilisateurs légitimes d'utiliser le site jusqu'à la neutralisation de l'attaque, génèrent des coûts financiers et entachent la réputation de l'entreprise.

Un CIAM sécurisé par Okta

> « En matière de sécurité, il faut toujours penser en termes de risque. Il n'existe pas de solution de sécurité universelle, adaptée à tous les scénarios. Vous devez prendre les décisions de sécurité en fonction des risques propres à votre entreprise, à vos clients et à vos utilisateurs. Vous pouvez renforcer ou assouplir vos contrôles de sécurité en conséquence. Cela vous permettra de ne pas trop alourdir la sécurité de votre produit afin de ne pas nuire à sa fluidité. »
>
> **Duncan Godfrey**
> Vice President, Security Engineering, Okta

M. Godfrey insiste sur le fait que la sécurité est une cible mobile. Pour neutraliser efficacement les menaces pour la sécurité décrites dans le présent document, ainsi que celles qui séviront à l'avenir, il convient de recourir à une solution CIAM robuste, évolutive et extensible afin de trouver le juste équilibre entre sécurité, confidentialité et expérience client.

Du fait de sa position unique au niveau de la porte d'entrée numérique de votre entreprise, le CIAM est également à l'avant-poste de vos défenses du périmètre. C'est l'endroit où les cybercriminels concentrent leurs efforts, ainsi que le premier point de contact de vos clients pour entrer en interaction avec votre entreprise ou effectuer des achats. C'est à partir de là que vous régissez, analysez et stockez en toute sécurité les données de ces clients.

La modularité devient la norme en matière d'assemblage d'application. Les systèmes de paiement, de messagerie et d'authentification sont les principaux modules intégrés dans les outils SaaS. L'enquête d'Auth0 montre que 83 % des applications modernes en cours de développement exigent une authentification, alors que seulement 58 % des personnes interrogées déclarent utiliser un outil SaaS tiers. Tandis que votre équipe de développement s'emploie à élaborer le meilleur produit possible, les raisons ne manquent pas de confier à l'équipe Okta le soin de vous fournir la solution CIAM la plus performante et sécurisée.

> Pour que votre équipe de sécurité puisse identifier les attaques le plus précocement possible, raccourcir le délai d'intervention et prévenir les graves répercussions d'une compromission, elle a besoin d'informations en temps réel.

Normes ouvertes

Comme n'importe quel outil de cybersécurité, une solution CIAM peut s'appuyer sur des normes ouvertes ou être aussi fermée qu'une boîte noire. Dans ce dernier cas, vous dépendez entièrement du fournisseur, car ce dernier est le seul à avoir accès au backend de son système. Vous affranchir de cette dépendance vous laisse libre d'installer les fonctionnalités de sécurité de votre choix et de les compléter facilement en fonction de vos besoins (voir ci-dessous).

Des normes ouvertes, telles que OAuth2, OpenIDConnect et SAML, nous permettent de donner la priorité à une expérience client d'excellence, sans pour autant négliger l'aspect développement. Lorsqu'un visiteur peut créer un nouveau compte en quelques secondes en utilisant ses propres identifiants, l'expérience utilisateur s'améliore sensiblement. Il peut ainsi utiliser des mots de passe plus forts et moins nombreux et avoir l'esprit tranquille sachant que ses données sont stockées en toute sécurité par son fournisseur d'identité au lieu d'être réparties entre plusieurs systèmes.

Extensibilité

Pour fournir une solution à la fois flexible et évoluant en fonction des besoins métier de vos clients, il faut pouvoir ajouter ou personnaliser des fonctionnalités de façon simple et rapide. Pour ce faire, Okta permet à vos utilisateurs de trouver le juste équilibre grâce aux règles. Ces règles permettent notamment de créer un déclencheur en cas de « déplacement impossible ». Lorsqu'un utilisateur basé à Paris essaie de se connecter depuis le Brésil, l'utilisateur qui effectue une tentative de connexion au Brésil va recevoir un message MFA, contrairement à l'utilisateur basé à Paris dont l'identité a déjà été vérifiée. Les règles peuvent être également utilisées pour avertir d'autres systèmes d'événements de connexion dans le cadre d'une surveillance des événements ou de services clients.

Pour vos développeurs, l'écosystème de partenaires Okta est la clé de notre extensibilité. Si vous avez besoin d'une fonctionnalité qui ne fait pas encore partie de notre offre de base, c'est sans doute parce que nous proposons une intégration avec un acteur majeur du secteur disponible sur notre marketplace. Si vous avez besoin d'une fonctionnalité de gestion du consentement pour vous conformer aux nouvelles réglementations, il existe une intégration qui vous permettra d'en bénéficier.

Log streaming

Pour bénéficier d'un niveau de sécurité élevé, vous devez être en mesure d'utiliser les données générées par vos outils de cybersécurité. Le log streaming envoie aux entreprises disposant d'une infrastructure de données, des données en temps réel directement de la solution CIAM vers les solutions existantes de gestion des informations et événements de sécurité (SIEM) ou d'orchestration de la sécurité, d'automatisation et de réponse (SOAR). Ces solutions sont également importantes pour assurer votre conformité aux exigences de reporting et d'effacement stipulées par les réglementations en matière de sécurité des données susmentionnées.

Le marketplace Okta propose des intégrations avec Splunk, Sumo Logic et Datadog, entre autres. Votre équipe peut également élaborer une intégration personnalisée en utilisant nos API et notre bibliothèque SDK. Pour que votre équipe de sécurité puisse identifier les attaques le plus précocement possible, raccourcir le délai d'intervention et prévenir les graves répercussions d'une compromission, elle a besoin d'informations en temps réel.

Protection contre les attaques par force brute

Lors des attaques par force brute dans leur forme la plus simple, le cybercriminel essaie plusieurs mots de passe courants afin d'accéder à un compte utilisateur unique. Cette attaque en apparence simpliste peut être couronnée de succès, même si elle manque un peu d'efficacité, ce qui explique sa longévité. Si Okta détecte plus de 10 tentatives de connexion à un compte donné provenant de la même adresse IP, la protection contre les attaques par force brute bloque cette adresse IP pour le compte utilisateur ciblé (les autres comptes au même emplacement bénéficieront encore d'un accès) et envoie à l'utilisateur une alerte par e-mail. L'utilisateur concerné pourra débloquer l'adresse IP à partir de cet e-mail ou n'aura qu'à changer de mot de passe pour obtenir un déblocage automatique.

Détection des bots

Le blocage d'attaques de type credential stuffing plus complexes est impossible sans une fonctionnalité de détection des bots. Grâce aux données de nos 4,5 milliards de connexions mensuelles associées à une analyse des facteurs de risque, la fonction de détection des bots d'Okta permet d'identifier les tentatives de connexion susceptibles de provenir d'un botnet ou d'un script, et d'ajouter le cas échéant une étape CAPTCHA au flux. Les études réalisées par Auth0 montrent que cette

fonctionnalité permet de réduire l'efficacité d'une attaque credential stuffing de jusqu'à 85 %. Pour les utilisateurs légitimes qui se connectent à partir d'adresses IP connues et validées, cette étape de sécurité supplémentaire n'est pas nécessaire, ce qui permet de conserver la fluidité du flux de connexion pour les véritables utilisateurs. La limitation des risques combinée à la réduction des points de friction pour les utilisateurs légitimes permet de trouver le juste équilibre entre sécurité et expérience client, pour votre entreprise et vos clients.

Authentification multifacteur (MFA) adaptative

Le NIST (National Institute of Standards and Technology) intègre le MFA dans la liste des bonnes pratiques et recommande son utilisation systématique. Selon l'OWASP (Open Web Application Security Project), le MFA est « de loin la meilleure protection contre la majorité des attaques ciblant les mots de passe ». Okta Adaptive MFA améliore encore l'expérience utilisateur et la sécurité des données en ce domaine. À partir de repères contextuels, comme l'emplacement, l'identifiant unique du terminal, le délai depuis la dernière connexion, etc., la solution procède à une analyse des risques sur chaque événement de connexion utilisateur et demande d'autres facteurs uniquement si elle le juge nécessaire, comme dans le cas dans l'exemple de déplacement impossible ci-dessus.

Authentification sans mot de passe

Compte tenu des risques posés par les mots de passe, il serait peut-être temps de les éliminer du flux de connexion de vos clients. Grâce à Okta Passwordless, c'est possible. Le mot de passe est remplacé par un code à usage unique envoyé à l'utilisateur par e-mail ou SMS. L'élimination des mots de passe permet de réduire le risque d'attaques credential stuffing et d'autres formes de compromission de compte. Comme avec une API publique qui comprend des limiteurs de débit, les données utilisateurs sont protégées contre les attaques de bots ou automatisées.

Une solution CIAM associe sécurité et fluidité des connexions

Vous et votre équipe êtes suffisamment occupés à assurer la continuité des opérations de votre entreprise. Grâce à la modularisation et à l'intégration de solutions SaaS tierces, le cas échéant, l'implémentation d'une solution CIAM est rapide et sûre. Pour assurer ce niveau de sécurité tout en préservant la satisfaction des clients, il faut prendre en compte le fait que l'augmentation du nombre d'utilisateurs légitimes entraîne inévitablement une augmentation du nombre de cybercriminels ciblant vos données. Une solution CIAM tenant compte de cette dynamique peut faire évoluer le niveau de protection parallèlement au nombre d'utilisateurs.

Les entreprises sont de plus en plus attentives à la conception de leurs identités numériques. La gestion de l'expérience client dès la page de connexion est essentielle à l'établissement d'une relation de confiance.

Découvrez les avantages potentiels d'Okta Customer Identity pour votre entreprise grâce à notre calculateur du ROI.