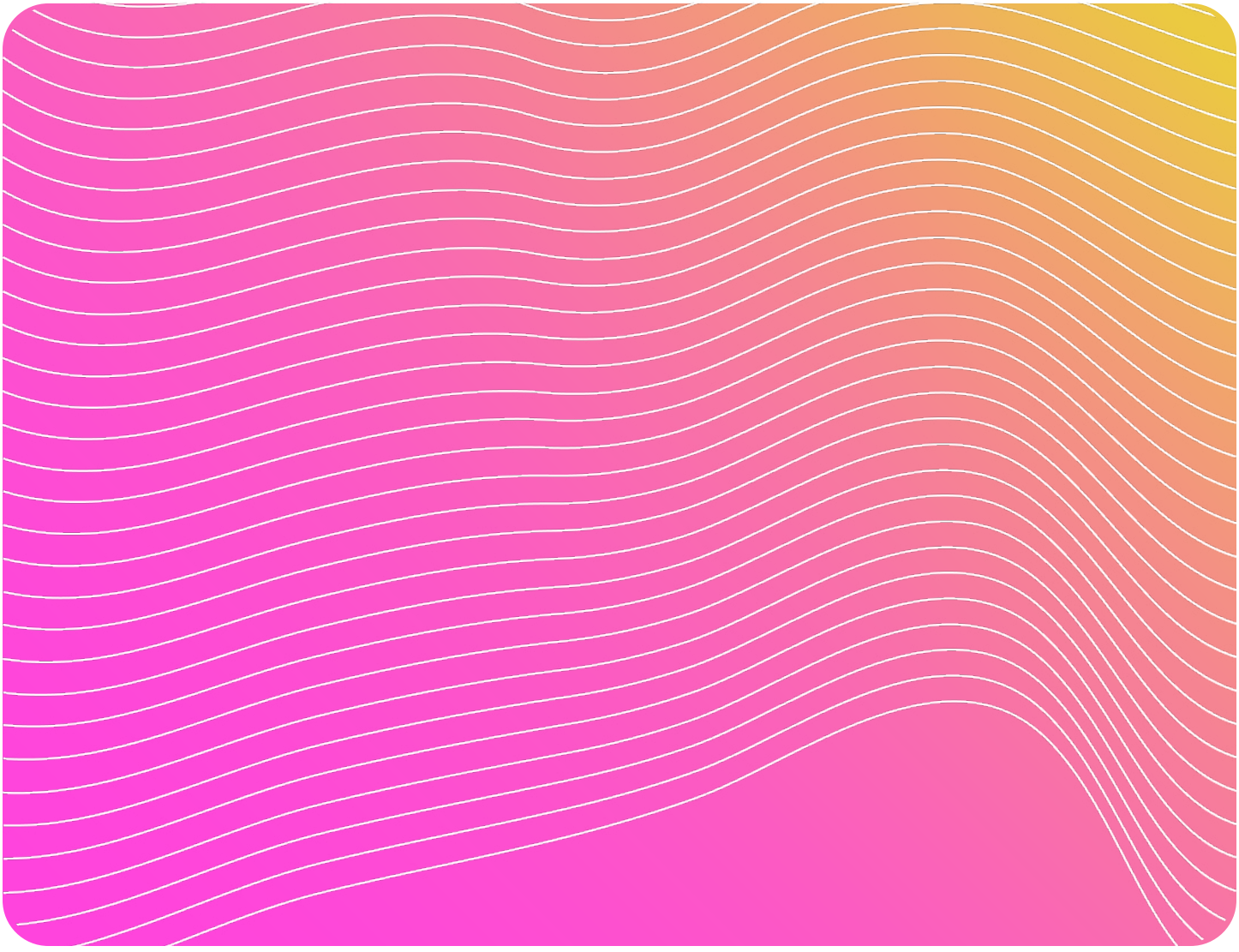
auth0

La CIAM (Gestion des identités et des accès clients) est l'outil idéal pour trouver le bon équilibre entre sécurité et expérience client

La sécurité est une cible mouvante.
Une solution CIAM performante vous aidera à concilier vos besoins et ceux de vos clients.



LIVRE BLANC

auth0.com

Avez-vous verrouillé la porte d'entrée ?

Il se passe souvent beaucoup de choses à ce moment-là. Vous devez jongler avec des paquets, les enfants vous accueillent, le téléphone sonne et le chat qui vous talonne. Il est assez facile de se perdre dans ce tourbillon et d'oublier une chose essentielle, comme verrouiller la porte. On a compris, la vie peut ressembler à une course.

Il en va de même pour la vie professionnelle, souvent en pire. Vous êtes en plein sprint, les derniers résultats du groupe de discussion avec les clients sont arrivés. Votre chef de projet essaie d'organiser une réunion pendant votre pause déjeuner et vous êtes sur le point de manquer une réunion debout. Si l'on ajoute à cela la vitesse toujours plus grande de l'adaptation numérique dans tous les secteurs et les effets persistants de la pandémie de COVID-19, les choses ne peuvent que s'accélérer.

En fait, Twilio rapporte que la puissante combinaison des efforts préexistants et de la dynamique provoquée par la pandémie a permis à de nombreuses organisations de voir leur transformation s'accélérer **de six ans en moyenne**, voire 10 ans dans certains secteurs. Dans cette enquête, 97 % des décideurs d'entreprise pensent que la pandémie est responsable de cette accélération. Afin de gérer cette adoption omnicanal à grande vitesse pour vos clients, vous devez réaliser qu'un système de gestion des utilisateurs unique et unifié est nécessaire pour votre prochaine version.

> **« La CIAM (Gestion des identités et des accès clients) est la solution qui vous permet d'intégrer, d'organiser et de gérer les comptes et les données des utilisateurs à partir d'un emplacement centralisé unique. »**

La page de connexion est la porte d'entrée de vos clients. Et c'est la première chose qu'ils voient ! Le flux de connexion doit donc leur offrir une excellente expérience utilisateur. Mais c'est aussi la première cible que choisissent de nombreux pirates à la recherche d'une vulnérabilité à exploiter. Cette page doit donc être parfaitement sécurisée. Il vous incombe donc de déterminer le niveau

de sécurité. Alors préférez-vous laisser la porte entrebâillée pour accueillir tous les invités, sans exception ? Ou bien ajoutez-vous des pênes dormants et une chaîne pour que chacun soit obligé de frapper et d'attendre que quelqu'un vienne et l'autorise à entrer ? Alors, sécurité laxiste et n'importe qui peut entrer, ou trop de sécurité et personne n'aura envie d'entrer ? La question est donc de trouver le bon équilibre entre sécurité et expérience client.

La CIAM (Gestion des identités et des accès clients) est la solution qui vous permet d'intégrer, d'organiser et de gérer les comptes et les données des utilisateurs à partir d'un emplacement centralisé unique. Un outil CIAM performant sert aussi à définir les mesures appropriées afin de préserver la sécurité des données de vos clients tout en garantissant aux utilisateurs une expérience sans friction.

En termes simples, les frictions entraînent des pertes de conversions, qu'il s'agisse d'un nouvel utilisateur qui abandonne au troisième CAPTCHA ou d'un client fidèle de longue date qui en a assez d'un flux de réinitialisation de mot de passe mal organisé. De tels exemples de friction dans le processus de connexion peuvent motiver des abandons de processus et des pertes d'utilisateurs. Ils en parleront à leurs amis, qui fuiront aussi votre entreprise. Cette publicité négative causera des dommages indicibles à votre marque à long terme.En tant que porte d'entrée numérique, la CIAM occupe une position unique au carrefour de la sécurité, de la confidentialité et de la facilité. Trouver la bonne combinaison de ces trois éléments fondamentaux pour votre produit et vos clients entraîne une complication possible, car engager des ressources de développement pour créer votre propre solution accaparera vos développeurs et vos ressources, au détriment de vos produits stratégiques. Votre équipe de développement est la meilleure dans son domaine. Ils utilisent leurs talents très étendus pour vous construire les meilleurs produits stratégiques. Pourquoi ne pas accorder le même niveau de compétences à l'expérience de connexion et à la sécurité des données de vos clients **avecl'aide des experts en gestion des identités**?

L'introduction d'une solution SaaS dédiée à la gestion des identités permet non seulement à vos développeurs de concentrer leurs talents sur le produit stratégique, mais elle garantit également que tout est mis en œuvre pour

sécuriser les informations de vos clients, ce qui contribue grandement à renforcer la confiance dans votre marque. Selon le rapport Trust Barometer 2020 d'Edelman, **La confiance et la réputation d'une marque** se placent en deuxième position (après le prix), parmi les facteurs de décision d'achat.

La CIAM vous permet de doser avec précision la sécurité, la confidentialité et la commodité

L'accélération de la transformation numérique dans tous les secteurs s'est accompagnée d'une augmentation des cyberattaques sur le périmètre de contact entre l'entreprise et le public. Pour de nombreux dirigeants, la protection de l'intégrité et de la réputation de la marque est donc passée au premier plan. Cela signifie que la protection de votre périmètre de contact client doit être une priorité stratégique. **Les violationsde données** peuvent causer des préjudices importants, non seulement réputationnels, mais aussi financiers, avec des ramifications potentielles pendant des années. Faire tout ce qui est en votre pouvoir pour prévenir tout risque d'attaque relève maintenant du bon sens commercial.

La plupart des entreprises dépendent des conversions, non ? Et comme les frictions entraînent des pertes de conversions, il est évident que tout effort de réduction des frictions sur la page de connexion ne peut qu'améliorer votre taux de conversion. La CIAM vous apporte la possibilité de contrôler l'expérience de connexion des clients et les données nécessaires pour continuer à faire évoluer cette expérience en fonction des besoins. En réglant les curseurs figuratifs de la sécurité, de la confidentialité et de l'expérience client pour obtenir le bon équilibre entre vos exigences et celles de vos clients, vous bénéficiez du niveau de sécurité dont vous avez besoin et l'expérience sans friction qu'ils exigent.

Cependant, la CIAM ne se contente pas de vous faire bénéficier d'une simple ouverture de session bien huilée. Une solution CIAM performante associe cette expérience utilisateur à une protection contre les cyberattaques, à la confidentialité des données des utilisateurs et à des contrôles intuitifs de la gestion des comptes utilisateurs.

Cette solution vous protège contre les vecteurs d'attaque courants en renforçant vos défenses périmétriques

Voyons un exemple avec ce scénario d'utilisation théorique : votre organisation développe sa présence sur le Web. Vous avez récemment acquis une startup de commerce en ligne ET vous avez terminé le développement d'un portail réservé aux membres pour leur proposer des offres exclusives pendant une seule journée, pour compléter vos applications et magasins Web existants. Votre équipe est chargée de regrouper tout cela dans une interface unifiée via une nouvelle application Web. C'est le moment idéal pour intégrer une solution CIAM extensible et évolutive qui permettra aux clients d'accéder à toutes les fonctions avec un seul jeu de coordonnées d'identification, réduisant ainsi votre surface d'attaque.

En outre, les solutions CIAM qui incluent des fonctionnalités telles que la détection des bots et les contre-mesures nécessaires, l'intégration de l'authentification multifacteur (AMF) et le flux des journaux d'événements contribuent à renforcer encore vos défenses. Dans le monde actuel de l'architecture distribuée, l'identité est le vrai périmètre de défense. L'extensibilité, l'évolutivité et les intégrations de partenaires sont essentielles pour déterminer si une solution CIAM permettra à votre entreprise de se développer tout en assurant la sécurité de votre périmètre et de vos données.

> **« En imposant des exigences minimales sur l'utilisation des mots de passe (avec des politiques de réutilisation), en rationalisant le flux de réinitialisation des mots de passe et en incluant l'AMF, la CIAM renforce votre périmètre d'identité. »**

La réutilisation des mots de passe est un des thèmes communs à de nombreux vecteurs d'attaque. En fait, une enquête récente de LogMeIn, fabricant du gestionnaire de mots de passe Lastpass, montre **quesi 91 % du public savent que la réutilisation** des mots de passe constitue un risque pour la sécurité, 66 % admettent qu'ils ignorent totalement cette mise en garde. La CIAM permet de

mieux appliquer les bonnes pratiques établies dans ce domaine. En imposant des exigences minimales sur l'utilisation des mots de passe (avec des politiques de réutilisation), en rationalisant le flux de réinitialisation des mots de passe et en incluant l'AMF, la CIAM renforce votre périmètre d'identité. »

Les données consolidées des utilisateurs sont plus faciles à protéger

SSoT (Single Source of Truth) est une infrastructure de gestion des données qui stipule que la situation idéale pour une entreprise est de stocker toutes les données pertinentes dans un référentiel centralisé, plutôt que de les garder dans plusieurs emplacements cloisonnés. La CIAM reprend ce concept et l'étend à vos données utilisateurs en rassemblant toutes les informations relatives aux comptes en un seul espace. Quel que soit le nombre de plateformes sur lesquelles vos applications finissent par résider, votre solution CIAM servira à gérer les comptes des utilisateurs et à acheminer toutes les données entrantes vers la même SSoT des identités.

Il est donc beaucoup plus facile de sécuriser et de blinder ces données, car il n'y a qu'un seul emplacement à protéger. La gestion centralisée des comptes utilisateurs joue aussi un rôle important pour la conformité aux principales réglementations sur la confidentialité des données. En vertu du RGPD européen et de la loi CCPA américaine, par exemple, les entreprises doivent fournir à la demande des copies des données personnelles d'un utilisateur ainsi que des informations sur leur utilisation. Et comme ces exigences s'étendent aux données et aux systèmes partenaires, la CIAM fournit l'accès facile dont vous avez besoin pour assurer la conformité, mais aussi et constamment la satisfaction de vos clients.

Votre SSoT des identités améliore également l'expérience de l'utilisateur. Grâce à l'authentification unique basée sur votre référentiel SSoT, les utilisateurs ont seulement à se souvenir d'un seul groupe de coordonnées d'identification. Cette satisfaction accrue rend moins probable l'abandon de votre application.

Cela signifie aussi des comptes orphelins en moins, vulnérables à une attaque ultérieure. Satisfaire pleinement toutes les parties prenantes n'est jamais une tâche facile. L'utilisation d'un outil modulaire CIAM SaaS peut vous rapprocher de cet idéal.

Des processus simplifiés pour satisfaire les utilisateurs

Chaque fois qu'un client crée un compte ou se connecte à un compte existant, il vous fait confiance. Les clients ont aussi confiance dans le fait que votre parcours client n'aboutira à des frustrations et autres motivations pour abandonner le processus. Lorsqu'ils découvrent que le processus mis en place ne leur impose que quelques étapes intuitives, et que leur accès est vérifié et autorisé très rapidement, que leur nouveau compte est prêt à fonctionner, vous leur avez démontré que leur confiance est justifiée.

Une solution CIAM devrait faire tout cela, en plus de rationaliser le processus de création de compte pour que les nouveaux utilisateurs se sentent bienvenus, tout en démontrant que vos procédures de traitement des données sont sécurisées. Selon PwC, **32 % des clients abandonnent un fournisseur** après une seule mauvaise expérience. Vous avez bien lu. Un tiers des personnes interrogées couperont définitivement les ponts avec une société après une seule expérience désagréable. Imaginez ce que ces personnes diront à leurs amis si cette mauvaise expérience était littéralement leur première rencontre avec votre entreprise ? Comme vous le verrez dans la section suivante, la CIAM peut apporter tous ces avantages dans vos processus et vos flux de comptes utilisateurs.

Un cycle de vie de l'utilisateur simplifié est plus facile à sécuriser

Des utilisateurs peuvent avoir d'autres raisons pour créer un nouveau compte. Par exemple, ils ont peut-être oublié leur mot de passe et trouvent que la procédure de réinitialisation du mot de passe est mal organisée. Bien entendu, cela se traduit

par un compte en double que vous devez maintenant gérer, tout simplement parce que vous ne savez pas qu'il s'agit d'un doublon. Tout au long du cycle de vie de l'utilisateur, une solution CIAM entièrement intégrée apporte des avantages clés en matière de sécurité.

Création de comptes

Afin d'éliminer les abandons de comptes, il est essentiel que le processus de leur création soit aussi simple que possible tout en vérifiant l'identité des utilisateurs. C'est exactement ce que font les solutions CIAM qui offrent une authentification unique. Permettre à un utilisateur de se connecter à votre service en ligne avec un compte de réseau social existant vous apporte la certitude que son identité a déjà été vérifiée. Et l'utilisateur peut créer son compte en quelques secondes.
Ce processus intuitif réduit la probabilité qu'un utilisateur réutilise son mot de passe, ce qui rend son compte plus difficile à pirater et renforce la protection de ses données.

Maintenance ces comptes

Pour la gestion générale des comptes d'utilisateurs, l'automatisation représente un atout incroyable. La CIAM devrait proposer un flux de réinitialisation automatique du mot de passe afin de limiter le niveau de friction de ce processus si souvent utilisé. Les options AMF qui résolvent les problèmes de contrôle d'identité des demandeurs d'accès constituent la prochaine étape d'une plateforme de gestion de compte complète. Grâce à la fédération de l'authentification des identités, lorsqu'un utilisateur crée accidentellement un compte en double, celui-ci est détecté et combiné à son autre compte dans votre SSoT des identités. La sécurité supplémentaire assurée par l'AMF et l'élimination des comptes dupliqués ou orphelins réduisent les possibilités de réussite des tentatives de violations.

Fin de vie des comptes

Que se passe-t-il lorsqu'un utilisateur néglige son compte ? Ou s'il passe à un autre produit, abandonnant complètement son compte ? Dans de nombreux cas, nous craignons qu'il ne se passe plus rien ! Sans une bonne hygiène des comptes, au fil du temps, votre SSoT des identités sera encombrée de comptes abandonnés, inutilisés et redondants. Il ne s'agit pas seulement d'un problème de maintenance, mais aussi de sécurité, car ces données d'identification peuvent être impliquées dans une violation de données quelque part et utilisées dans une attaque contre vos systèmes. Les fonctionnalités de compte automatisées, incluant les e-mails envoyés aux titulaires de comptes inactifs pendant une période prédéterminée, la désactivation automatique du compte et sa suppression éventuelle, permettant donc de bloquer ce vecteur d'attaque courant.

Les données d'identification des comptes violés ouvrent une variété de vecteurs d'attaques

Lorsque des données d'identification d'utilisateurs ont été volées pendant une attaque, elles peuvent être utilisées à plusieurs reprises pour accéder à de nombreux autres sites, surtout lorsque les mots de passe ne bénéficient pas d'une maintenance fiable. Les cybercriminels n'ont aucun mal à obtenir des noms d'utilisateur et des mots de passe, même s'ils n'ont pas les compétences techniques pour pénétrer dans une base de données… Ces débutants du piratage, qui méritent leur surnom de « script kiddies », se contentent d'acheter une « liste combo » de données d'identification sur le dark web. Ils utilisent des scripts préexistants ou des applications complètes, également disponibles sur le dark web, pour lancer une intrusion par bourrage de données d'identification ou une autre attaque de type force brute. Vous devez connaître ces vecteurs d'attaque et leurs méthodes si vous voulez intégrer votre CIAM de la meilleure façon possible en fonction de vos besoins.

Bourrage d'identifiants

L'un des vecteurs les plus répandus aujourd'hui est l'attaque en force brute connue sous le nom de **bourrage d'identifiants**. Ce type d'attaque exploite une liste de noms d'utilisateurs et de mots de passe et les injecte dans le flux de connexion d'un autre site. La prévalence des mots de passe réutilisés rend ce vecteur d'attaque remarquablement attrayant pour les hackers. En effet, les données d'identification fonctionnent au moins assez souvent pour en valoir la peine. Ces attaques profitent principalement de la paresse naturelle des gens, qui réutilisent des mots de passe trop basiques et donc faciles à pirater. **Les mots de passe les plus courants** sont actuellement « 123456 » et même « motdepasse », pas loin derrière.

Business Email Compromise (BEC)

Les données des mots de passe volés peuvent servir de fondations à d'autres attaques. Par exemple, un pirate peut acheter une liste combo provenant d'une organisation qu'il souhaite spécifiquement cibler. En extrayant les identifiants de connexion réseau de certains cadres supérieurs et en utilisant des techniques d'usurpation d'identité, ils envoient des e-mails d'hameçonnage ciblés (ou spear phishing) qui semblent provenir de ces personnes. Ces attaques de plus en plus fréquentes s'appuient sur des bots. Elles constituent avant tout un vecteur d'ingénierie sociale, dont le succès repose sur le facteur humain de la sécurité (ou plutôt son absence).

Attaques de bots

Certains pirates veulent simplement perturber en profondeur les systèmes de l'entreprise qu'ils ont ciblée. Le vol n'est pas leur intention. Ils veulent simplement se faire remarquer en interrompant des opérations et observer le chaos pendant que la victime tente d'arrêter l'intrusion et rétablir ses activités. Les attaques par déni de service distribué (DDoS) en sont l'exemple le plus courant : le pirate utilise des bots pour inonder un site de trafic. Il le rend ainsi inaccessible aux visiteurs légitimes pendant un certain temps. Ces attaques finissent par coûter cher à l'entreprise victime, tant en termes de réputation que de coûts financiers générés par l'interruption des services.

Une autre attaque de bots courante consiste à inonder le flux de connexion d'un site de commerce électronique afin d'acheter des articles très recherchés sur le marché. Des essaims de bots de ce type ont été récemment utilisés lorsque **Nvidia a lancé une nouvelle carte graphique** très attendue par les gamers du monde entier. Des techniques d'attaques similaires ont été utilisées lorsque Microsoft a lancé la X-Box X, et Sony sa très attendue Playstation 5. Des sites comme Walmart et Amazon ont vu leurs capacités de traitement considérablement affectées par des centaines de milliers de comptes créés par des bots et utilisés **pour s'emparer de tous les stocks disponibles** afin de

faire monter les prix sur le marché secondaire. Non seulement ces scénarios par vagues successives de bots limitent la disponibilité des produits, mais ils empêchent également les utilisateurs légitimes d'utiliser le site jusqu'à ce que l'attaque soit contrée et résolue. L'impact financier et réputationnel est évidemment considérable.

Auth0 et la sécurité de la CIAM

« Pour réfléchir aux questions de sécurité, vous devez toujours penser aux risques, aux conséquences. »
Il n'existe pas de solution de sécurité unique. Vos décisions doivent être déterminées par les risques spécifiques à votre entreprise, à vos clients et à vos utilisateurs. Vous pouvez ajuster à la baisse et à la hausse vos contrôles de sécurité en conséquence.
« Cela vous aidera réellement à ne pas complexifier inutilement la sécurité de votre produit, ce qui pourrait avoir un impact négatif sur sa facilité d'utilisation ».

DUNCAN GODFREY, DIRECTEUR PRINCIPAL DE L'INGÉNIERIE DE SÉCURITÉ, AUTH0

Duncan insiste sur le fait que la sécurité est une cible mouvante. Des efforts combinés sont nécessaires pour contrer des menaces de sécurité, comme celles évoquées ici et celles que les pirates n'ont pas encore dévoilées. Ces efforts incluent une solution CIAM robuste, développée pour être évolutive et extensible. Elle doit vous permettre de trouver le bon équilibre entre sécurité, confidentialité et expérience client.

En raison de sa position unique sur le portail d'accès numérique à votre organisation, la CIAM est en première ligne pour assurer vos défenses périmétriques. C'est là que les acteurs malveillants concentrent leurs efforts. C'est aussi le premier endroit que vos clients voient lorsqu'ils viennent interagir avec votre organisation ou faire un achat. C'est également sur cet espace que vous gérez, analysez et stockez en toute sécurité les données relatives à ces clients.

La modularité est déjà en train de devenir rapidement la norme de conception des applications, avec les systèmes de paiement, de messagerie et d'authentification en tête des outils SaaS en cours d'intégration. Les études d'Auth0 ont révélé que **83 % des applications modernes en cours de développement nécessitent une authentification**, mais que seulement 58 % des personnes interrogées déclarent utiliser un outil SaaS tiers. Pendant que votre équipe de développement s'investit dans la création du meilleur produit stratégique possible, vous pouvez pour de très bonnes et nombreuses raisons confier à notre équipe la responsabilité de vous fournir la meilleure solution CIAM et bénéficier ainsi de la sécurité la plus fiable possible.

> **Lorsque votre équipe de sécurité a toutes les données les plus récentes, les attaques peuvent être détectées avec une précocité optimale. Les temps de réponse deviennent alors plus courts et vous évitez d'importantes retombées générées par d'éventuelles violations.**

Normes ouvertes

Comme tout autre outil de cybersécurité, une solution CIAM peut adhérer à des normes ouvertes ou fonctionner comme une « boîte noire ». Dans ce dernier cas, vous êtes dépendant du fournisseur puisque lui seul a accès au back-end de son système. C'est ce que l'on appelle l'« enfermement propriétaire ». Lorsque vous pouvez l'éviter, vous gardez toute votre agilité pour mettre en œuvre votre sécurité et bénéficier d'une extensibilité facile (voir ci-dessous).

Les normes ouvertes telles que OAuth2, OpenIDConnect et SAML sont au cœur de notre approche pour mettre l'expérience client au centre de nos activités, tout en maintenant la focalisation de nos développeurs. Lorsqu'un visiteur peut créer un compte en quelques instants à l'aide des données d'identification qu'il possède déjà, son expérience utilisateur s'améliore considérablement. Cela lui permet d'utiliser des mots de passe renforcés et moins nombreux. Chaque utilisateur peut avoir l'esprit tranquille en sachant que ses données sont stockées en toute sécurité chez son fournisseur d'identité, au lieu d'être dispersées dans plusieurs systèmes.

Extensibilité

Pour offrir une solution capable de s'adapter aux besoins de vos clients, il est indispensable de pouvoir ajouter et personnaliser des fonctionnalités avec rapidité et en toute transparence. Les règles sont l'une des méthodes mises au point par Auth0 pour offrir de tels avantages et permettre à vos utilisateurs de trouver l'équilibre dont ils ont besoin. Elles servent par exemple à créer des déclencheurs pour activer des scénarios de « parcours impossibles ». Lorsqu'un utilisateur tente d'accéder au système depuis le Brésil, il reçoit une invite AMF. Un utilisateur à Chicago qui tente de se connecter depuis le Brésil ne verra pas cette invite, si son identité a déjà été authentifiée. Nos règles servent aussi à partager des événements de connexion avec d'autres systèmes, pour assurer le suivi des événements ou de service à la clientèle.

Pour vos développeurs, l'écosystème des partenaires d'Auth0 est la clé de notre extensibilité. Si vous avez besoin d'une fonctionnalité qui n'est pas encore incluse dans notre offre de base, il est très probable que vous la trouverez intégrée par un leader du secteur disponible sur notre Marketplace. Lorsque vous avez besoin de gérer des consentements afin de rester en conformité avec les nouvelles réglementations, nous avons une intégration pour répondre à cette exigence.

Flux des journaux

La capacité d'exploiter les données générées par vos outils de cybersécurité est l'une des caractéristiques d'une solide posture de sécurité. Pour les organisations qui ont mis en place une infrastructure de données, le flux des journaux envoie les données CIAM en temps réel directement aux solutions SIEM (Gestion des événements et des informations de sécurité) ou SOAR (Orchestration, automatisation et réponse aux incidents de sécurité informatique) existantes. Cet aspect est également essentiel pour la conformité aux exigences de notification et d'effacement prévues par les règlements sur la sécurité des données susmentionnés.

Marketplace Auth0 Il inclut les intégrations avec Splunk, Sumo Logic, Datadog et d'autres. Votre équipe peut créer une intégration personnalisée à l'aide de nos nombreuses API et de notre bibliothèque de SDK. Lorsque votre équipe de sécurité dispose de toutes les données les plus récentes, les attaques peuvent être détectées avec une précocité optimale. Les temps de réponse deviennent alors plus courts et vous évitez d'importantes retombées générées par d'éventuelles violations.

Protection contre les attaques en force brute

Dans leur forme la plus simple, les attaques en force brute consistent à essayer plusieurs mots de passe courants pour tenter d'accéder à un seul compte utilisateur. Cette attaque apparemment peu sophistiquée peut réussir, en dépit de son inefficacité, ce qui explique sa popularité continue. Si Auth0 détecte plus de 10 tentatives de connexion pour un compte donné avec la même adresse IP, la protection contre la force brute bloquera cette IP pour le compte utilisateur ciblé (tous les autres comptes au même endroit disposeront encore d'un accès) et enverra à l'utilisateur concerné un e-mail d'alerte. L'utilisateur concerné pourra débloquer l'IP à partir de cet e-mail ou celle-ci sera automatiquement débloquée après modification du mot de passe.

Détection des bots

Lorsqu'il s'agit d'arrêter des attaques plus complexes par bourrage d'identifiants, la détection des bots est souvent le chaînon manquant. En utilisant les données fournies par nos 4,5 milliards de connexions mensuelles combinées à l'analyse des signaux de risque, la détection des bots Auth0 peut identifier les tentatives de connexion susceptibles de provenir d'un botnet ou d'un script et injecter une étape CAPTCHA dans le flux. Les études d'Auth0 ont montré que cela **peutréduire de 85 % l'efficacité d'une attaque par bourrage d'identifiants**. Pour les utilisateurs légitimes qui se connectent à partir d'adresses IP connues, par exemple, cette étape de sécurité supplémentaire n'est pas nécessaire, ce qui

permet aux clients authentiques de bénéficier d'un flux sans friction. L'atténuation des risques et la réduction des frictions pour les utilisateurs authentiques font partie de notre concept pour vous aider à trouver le bon équilibre entre sécurité et expérience client pour vous et vos clients.

Authentification multifacteur adaptative - AMF

Le National Institute of Standards and Technology (**NIST**) considère que l'AMF est une bonne pratique et **recommande son utilisation** généralisée. Et selon le groupe industriel Open Web Application Security Project (**OWASP**), l'AMF est « de loin la meilleure défense contre la majorité des attaques associées aux mots de passe ». **Authentification multifacteur adaptative Auth0** porte l'AMF à un niveau supérieur d'expérience utilisateur et de sécurité des données. Grâce à des indices contextuels, tels que la localisation, l'identifiant unique de l'appareil, le temps écoulé depuis la dernière connexion, etc., l'authentification multifacteur adaptative d'Auth0 lance une analyse de risque sur chaque événement de connexion des utilisateurs. Elle déclenche une demande de facteurs supplémentaires uniquement lorsque cela est jugé nécessaire, comme dans notre exemple de parcours impossible ci-dessus.

Authentification sans mot de passe

Compte tenu des problèmes liés aux mots de passe, il est peut-être temps de permettre à vos clients de les supprimer complètement du flux de connexion. Avec Auth0 Passwordless, c'est exactement ce que vous pouvez faire, en substituant un code à usage unique envoyé à l'utilisateur par e-mail ou par SMS. Grâce à l'élimination des mots de passe, vous atténuez l'exposition aux attaques par bourrage d'identifiants et à d'autres formes de corruption de comptes. Et avec une API publique qui intègre des limiteurs de débit, les données des utilisateurs sont également protégées contre les attaques automatisées ou par bots.

La CIAM assure la sécurité et gère les frictions de connexion

Vous et votre équipe avez suffisamment de choses à faire pour rester occupés jusqu'à votre prochain sprint ! Avec la tendance à la modularisation et l'intégration des solutions SaaS tierces lorsque cela est possible, vous pouvez mettre en œuvre votre solution CIAM avec rapidité et en toute sécurité. Pour assurer cette sécurité et maintenir la satisfaction client, il est impératif de comprendre que toute augmentation du nombre d'utilisateurs légitimes s'accompagne d'une augmentation simultanée du nombre de personnes malveillantes qui tentent de s'emparer de vos données. Une solution CIAM qui intègre cette dynamique devient capable de faire évoluer la protection en même temps que le nombre d'utilisateurs.

Les entreprises se focalisent de plus en plus sur les options de création des identités numériques. La gestion de l'expérience client dès la page de connexion joue un rôle essentiel pour créer des relations de confiance. Si vous estimez qu'il est temps pour votre entreprise d'accorder plus d'attention à votre solution de gestion des accès, **prenez contact avec notre équipe de spécialistes de la sécurité des identités** dès aujourd'hui, pour amorcer une conversation.

À propos d'Auth0

Auth0, un pôle de produits au sein d'Okta, adopte une approche moderne de l'identité et permet aux organisations de fournir un accès sécurisé à n'importe quelle application, pour n'importe quel utilisateur. La plateforme d'identité Auth0 est hautement personnalisable, et répond aux besoins des équipes de développement en termes de simplicité d'utilisation et d'adaptabilité. En protégeant des milliards de transactions de connexion chaque mois, Auth0 offre confort, confidentialité, et sécurité, pour permettre aux clients de se concentrer sur l'innovation.

Pour plus d'information, rendez-vous sur **https://auth0.com/fr**