Livre blanc

Le vrai coût d'une solution d'identité interne

okta

Introduction

Vous avez certainement déjà envisagé de créer en interne votre propre solution de gestion des identités. Cependant, le coût d'une telle initiative peut se révéler astronomique si vous ne mettez pas en place une stratégie appropriée. Par exemple, n'avez-vous jamais demandé à votre équipe technique de créer une solution d'identité, puis de devoir changer votre infrastructure ou de voir la réglementation évoluer au bout de quelques mois ? Rassurez-vous, de nombreuses entreprises sont dans votre cas.

Ce phénomène, qui n'est pas unique dans le secteur technologique, s'accompagne d'une évolution constante des vecteurs d'attaque. Autrement dit, la prévention des fraudes est une activité plus stratégique que jamais, et de plus en plus difficile à mener à bien. De plus, les entreprises doivent assurer la conformité lors du traitement des données clients et de la protection des services, mais elles disposent souvent d'un délai limité pour déployer des mises à jour dans leur environnement.

Si une solution de gestion des identités clients (CIAM) adaptée permet généralement de relever tous ces défis, la création en interne de ce type de solution peut provoquer plus de problèmes qu'elle n'en résout. Nous vous expliquons pourquoi en quelques points :

Le coût d'une équipe entièrement dédiée à l'identité

L'équipe DevSecOps est chargée de répondre aux besoins MDR (Managed Detection and Response) et XDR (eXtended Detection and Response) d'une entreprise. Mais en général, les entreprises qui utilisent des systèmes hérités laissent l'équipe technique[1] déterminer les rôles et responsabilités des responsables des applications et des professionnels de la sécurité.

Les technologies d'identité font souvent les frais de la confusion qui en résulte, car les solutions CIAM créées en interne sont généralement conçues au niveau des applications. En outre, la gestion des identités clients impose une forte charge aux équipes DevSecOps, car une collaboration supplémentaire est nécessaire entre les différentes équipes techniques pour sécuriser efficacement les applications clients et les déploiements de points de service.

Cette collaboration peut s'avérer coûteuse et, sans un accès automatisé permettant un provisioning au cas par cas, un contrôle des accès basé sur les rôles et une mise en production à flux tendu (JIT), les délais de déploiement sont rallongés et la surveillance n'est pas exhaustive.

En plus, le DevSecOps devient plus agile – et l'accélération de la transition vers le cloud exige des investissements stratégiques dans les outils appropriés[2] pour évaluer les risques au fil des différents processus et frameworks du flux d'intégration et de distribution continues (CI/CD).

Il faut cependant savoir que les environnements cloud optimisés peuvent améliorer d'environ **38 %** la productivité de la maintenance et réduire de près de **29 %** les coûts d'infrastructure pour les applications migrées[3]. Ces économies représentent un capital significatif que les entreprises peuvent réinvestir dans des opérations stratégiques.

[1] Why your security risk management program should include legacy systems, Infosec

[2] The Best IAM Practices for DevOps, DevOps.com

[3] Cloud's trillion-dollar prize is up for grabs, McKinsey

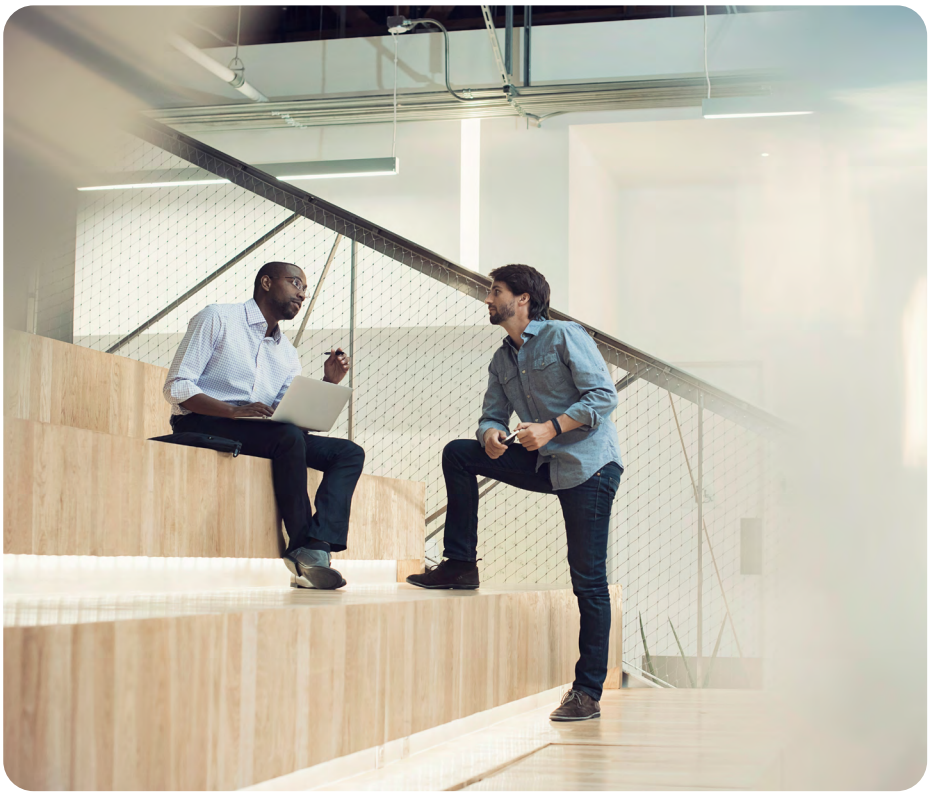
Coût en hausse du déficit technique

L'implémentation d'une authentification optimisée, appliquant des normes de sécurité fortes sur une multitude d'applications et de ressources, est une tâche sans fin. Le provisioning manuel des utilisateurs ne nécessite pas seulement des investissements opérationnels intensifs, mais dans le cas de systèmes complexes ou dynamiques, il peut également donner lieu à des accès inappropriés (c'est-à-dire trop permissifs).

De même, il peut arriver facilement qu'une solution développée en interne collecte trop de données ou spécifie des demandes faisant fi des spécificités d'accès, ce qui ouvre la porte aux activités malveillantes.

En plus d'accroître le risque d'erreur humaine, la gestion des identités clients en interne nécessite aussi une maintenance constante et un traitement rigoureux. Plus l'empreinte numérique est étendue, plus la surface d'attaque l'est également[4], et il suffit à un acteur malveillant d'accéder à un seul compte pour provoquer une brèche de données. Sans compter qu'avec l'arrivée prochaine de l'informatique quantique[5], les services de chiffrement internes seront encore plus vulnérables au vol de données.

En déléguant la responsabilité des identités clients à un fournisseur de confiance, les entreprises peuvent rapidement gagner en sérénité, car elles bénéficient de protocoles de sécurité efficaces qui assurent une protection contre l'activité IA malveillante.



[4] Securing The Future: The Most Critical Cybersecurity Trends Of 2023, Forbes

[5] A game plan for quantum computing, McKinsey

Le traitement conforme des données se fera sans cookies

Nous savons désormais que nos informations personnelles sont diffusées sur Internet, et les acteurs technologiques, les organismes de réglementation et les utilisateurs se sont attelés à la tâche de faire évoluer les pratiques de données actuelles afin de les rendre plus transparentes et modérées par les consommateurs.

La collecte de cookies tiers a longtemps été indispensable pour personnaliser les expériences, mais elle pose de façon inhérente des problèmes de confidentialité, en particulier concernant le consentement des utilisateurs et la propriété des données. Cependant, les cookies sont en train de disparaître progressivement[6], ce qui entraîne de nombreuses conséquences sur la façon dont les entreprises collectent et échangent les informations de leurs clients, ainsi que sur la création des profils clients.

Les utilisateurs ont aujourd'hui davantage de discernement quant aux applications avec lesquelles ils partagent leurs données[7], et la réglementation soutient les consommateurs en obligeant les entreprises à agir pour développer la confiance en leur marque via une stratégie sans cookies.

> 27 % des leaders technologiques indiquent que leur principal défi est d'assurer la conformité de leurs processus de collecte des données avec la réglementation en matière de confidentialité et de sécurité[8]
>
> – **Étude Kantar/Okta**

Pour relever ces défis, de nombreuses entreprises choisissent désormais d'externaliser leur solution CIAM à des fournisseurs de confiance qui offrent des fonctionnalités prêtes à l'emploi sophistiquées. Avec le progressive profiling, par exemple, les utilisateurs peuvent indiquer les informations qu'ils acceptent de partager avec vous, sans cookies et sans que vous deviez ajouter de ressources techniques pour respecter les exigences de conformité.

[6] The Slow Death Of Third-Party Cookies, Forbes

[7] The mismanagement of user consent data and its consequences, iapp

[8] The Future is CIAM: Insights from 200 APJ leaders, Okta

Fidéliser les clients en suivant l'évolution du marché

À première vue, la proposition de valeur suivante semble relativement simple : plus la connexion et l'accès au paiement sont rapides pour le client, plus le taux de conversion sera élevé[9]. La réalité est plus nuancée, cependant, car les avis divergent quant au concept même de friction et aux moyens de la réduire tout en préservant la sécurité lors de l'authentification et de l'autorisation des utilisateurs.

La confiance en une marque ne signifie pas simplement de collecter des données zero party au moment de la création du compte et de la connexion, mais aussi de tout mettre en œuvre pour faire en sorte que vos clients profitent d'une expérience de connexion sécurisée[10].

Si une solution d'identité interne ne permet pas vraiment de résoudre ces problèmes, les entreprises ayant investi dans des solutions CIAM dans le cloud bénéficient déjà de leurs avantages de façon globale. En plus d'offrir des expériences clients sur mesure[11] qui donnent le choix de la méthode d'authentification, ces solutions se conforment également aux dernières normes de confidentialité et de sécurité, augmentent les conversions grâce à des expériences optimales et donnent aux équipes techniques les moyens d'innover.

[9] Conversion Rate Optimization – It's a Journey, Not A Destination, Customer Think

[10] Access management must get stronger in a zero-trust world, Venturebeat

[11] The Benefits Of Passwordless Authentication And How To Choose The Right Method, Forbes

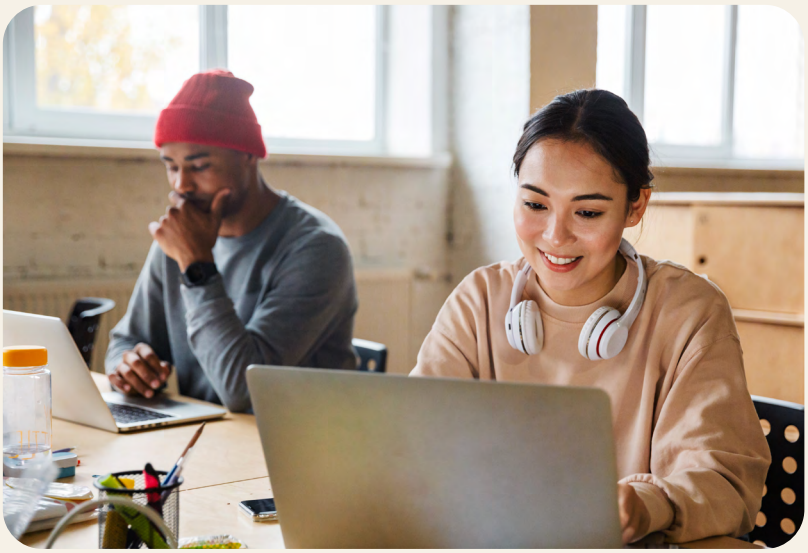
Pourquoi Okta ?

Le CIAM est conçu pour prendre en compte les changements et s'adapter à l'évolution des frameworks. De fait, les entreprises qui anticipent les besoins de leurs clients et déploient rapidement les solutions adaptées sont celles qui tirent leur épingle du jeu.

Une solution CIAM efficace comme celle d'Okta non seulement permet de trouver un équilibre entre innovation et sécurité, mais peut aussi être intégrée en un clic à vos nombreux services et applications à mesure que votre activité se développe. Avec des fonctionnalités telles que la notification des brèches, la protection contre les attaques multiniveau et l'orchestration disponible dès le premier jour, nous pouvons aussi vous aider à mieux sécuriser vos applications et services, et à en savoir plus sur vos clients.

Enfin, en intégrant les dernières normes en matière d'identité et de sécurité, Okta Customer Identity Cloud offre une solution complète qui a déjà aidé de nombreuses entreprises à accélérer l'innovation tout en offrant une expérience numérique plus sûre, plus rapide et plus pratique à leurs clients.

Pour découvrir comment Okta Customer Identity Cloud peut aider votre entreprise, consultez notre livre blanc **Développer ou acheter**.



Livre blanc

Le vrai coût d'une solution d'identité interne

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie
+33 01 85 64 08 80