IBM Security

Rassembler les parties prenantes pour moderniser le CIAM dans l'ensemble de l'organisation

IBM

Lancez-vous

Introduction

Lorsque vous créez un nouveau compte, effectuez un achat ou même lorsque vous vous inscrivez à une newsletter, vous confiez vos informations personnelles à une organisation. Après cet échange initial, vous ne souhaitez probablement pas que vos informations soient utilisées à des fins autres que celles que vous avez acceptées, mais avec votre consentement, vous apprécierez peut-être des expériences personnalisées et des recommandations pour l'avenir. Le plus important dans tout cela, c'est que la balle est dans votre camp : libre à vous de changer d'avis à tout moment. Si jamais vous rencontrez des frictions au cours de vos interactions ou si vous commencez à perdre confiance dans l'organisation pour une raison quelconque, vous l'abandonnerez probablement et en trouverez une autre.
La gestion des identités et des accès des consommateurs (CIAM) permet ces expériences à la demande, personnalisées et fiables entre les consommateurs et la marque, et en tant que consommateur, vous pouvez sympathiser avec vos propres consommateurs lorsque vous envisagez des mises à jour des stratégies numériques de votre organisation pour rester compétitif.

Toutefois, CIAM est bien plus qu'une mise à jour de site Web ou un projet de marketing ; il a des répercussions sur les domaines fonctionnels de l'organisation à mesure que les points de contact avec les consommateurs sont évalués et modernisés. Afin de veiller à ce que l'équilibre intemporel entre la commodité et la sécurité ne penche pas, les organisations doivent réunir les parties prenantes commerciales et techniques pour reconnaître le CIAM comme un sous-ensemble de la transformation numérique axé sur les résultats qui peut partager des composants technologiques avec l'IAM de la main-d'œuvre. Lorsqu'elles sont mises en œuvre de manière stratégique et ciblée, les organisations peuvent maximiser leur engagement avec les consommateurs tout en minimisant les risques pour le personnel informatique et de sécurité.

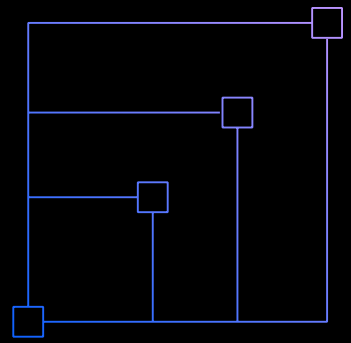
Sans stratégie CIAM, les entreprises risquent de perdre des revenus du fait de la défection des clients ; la fidélité à la marque reste fragile lorsque des alternatives sont disponibles à portée de main. De même, dans le secteur public, les agences gouvernementales qui s'agrippent encore en grande partie à l'infrastructure et aux processus hérités peuvent perdre la confiance de leurs citoyens et ne pas atteindre les niveaux idéaux d'adoption du service public.
En dépit des différences dans leurs missions, les secteurs privé et public sont liés par leur besoin de servir les consommateurs avec une expérience numérique conviviale mais sécurisée afin de faciliter le partage d'informations respectueux de la confidentialité. De nombreuses organisations ont pris note de faire exactement cela, faisant du CIAM le segment le plus important du marché total de l'IAM, un marché censé enregistrer une croissance de 15,1 %[1] par an jusqu'en 2025. Pour les gens qui n'ont pas encore entamé leur modernisation numérique, l'une des premières et des plus importantes étapes consiste à créer un alignement du leadership sur plusieurs rôles fonctionnels afin que tout le monde puisse bénéficier du projet.

Chief Marketing Officer – (CMO)

Objectif CIAM : capturer, encourager et développer les utilisateurs par le biais d'expériences personnalisées respectueuses de la confidentialité et contrôlées par l'utilisateur.

Dans l'ensemble du secteur privé, les spécialistes du marketing bataillent ferme pour attirer l'attention des clients potentiels, et ce qu'ils souhaitent éviter à tout prix, c'est qu'une expérience d'enregistrement difficile éloigne les clients à la dernière minute. La défection des clients peut avoir un impact direct sur les revenus, c'est pourquoi les programmes CIAM visent à rationaliser les expériences d'enregistrement et d'intégration pour éviter ce problème et convertir les prospects inconnus en opportunités commerciales. Les formulaires d'intégration idéaux demanderont le moins d'informations possible sur le client, avec des points de contact correctement configurés pour en savoir plus sur un client au fur et à mesure que la relation se développe.

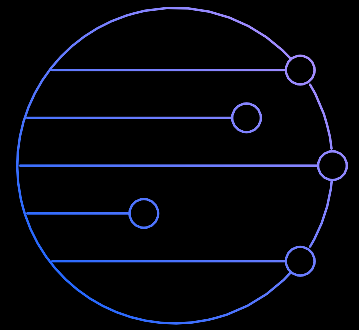
Les grandes organisations avec plusieurs sous-marques doivent structurer leurs magasins de données pour maintenir une identité unique pour chaque consommateur, en s'intégrant à la gestion de la relation client (CRM) et à d'autres outils et systèmes tiers en cours de route. Avec la centralisation des identités des consommateurs, la mise en œuvre stratégique des meilleures pratiques CIAM permettra aux spécialistes du marketing de mieux comprendre le comportement de leurs consommateurs et de mener des campagnes marketing plus ciblées et personnalisées. Le CIAM joue un rôle central dans l'expérience numérique des prospects et des clients, il est donc naturel que les responsables marketing jouent un rôle clé dans le processus de planification de la modernisation.



Responsables de secteurs d'activité

Objectif CIAM : offrir une expérience simplifiée et conviviale avec des interfaces modernes et un engagement pour permettre d'atteindre les objectifs de l'organisation

La direction générale ou les propriétaires d'agences sont également poussés à intégrer les consommateurs et à permettre des interactions aisées, mais pas nécessairement dans l'intérêt des revenus. Par exemple, les agences gouvernementales doivent fournir efficacement des services publics aux citoyens et moderniser l'engagement sur un vaste éventail de préférences et de canaux d'utilisateurs, généralement sans véritable fonction de marketing dans l'organisation. Les propriétaires d'agences recherchent une transformation similaire du parcours de l'utilisateur pour simplifier l'enregistrement et réduire les abandons afin d'assurer une prestation de services réussie. Bien qu'ils ne mènent peut-être aucune campagne marketing, ces chefs d'entreprise visent toujours à obtenir une identité unique pour chaque consommateur afin de rationaliser les interactions des consommateurs entre les départements, d'éliminer les redondances et de mieux comprendre le comportement.

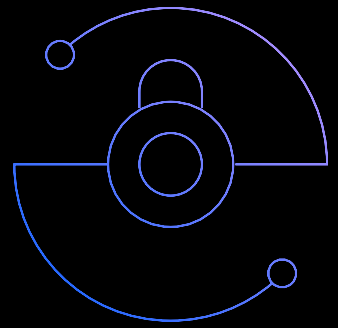


Agents de sécurité et de confidentialité

Objectif CIAM ; Offrir des interactions sécurisées avec les consommateurs pour empêcher la fraude des utilisateurs et la compromission des comptes, fournir des expériences transparentes et contrôlées par les utilisateurs et maintenir la conformité

Comme principe directeur, les consommateurs doivent savoir qui contrôle leurs données et comment elles sont utilisées, en ayant la possibilité d'utiliser leurs propres données en libre-service et de modifier leur consentement à tout moment. C'est une raison suffisante pour que les organisations donnent la priorité à la gestion de la confidentialité et du consentement pour leurs expériences numériques, mais les réglementations mondiales ajoutent une urgence forcée au problème. Les entreprises doivent se conformer aux règles de chaque région dans laquelle elles interviennent ou s'exposer à de lourdes pénalités et amendes, et bien que les lois sur la protection de la vie privée détaillent ce que les organisations sont tenues de faire, elles ne fournissent généralement pas d'instructions spécifiques sur la façon d'y arriver. Une implémentation CIAM appropriée agit comme une source unique de vérité pour toutes les informations personnellement identifiables (PII). Les responsables de la confidentialité et les experts en conformité peuvent définir des règles et des politiques à diverses fins de gestion du consentement que le personnel technique applique simplement aux applications nécessaires. Cela permet au personnel chargé de la confidentialité et de la conformité d'aller au-delà des feuilles de calcul et de répondre à la réalité dynamique des lois sur la confidentialité et de les rendre plus accessibles.

Bien que les RSSI partagent un intérêt pour la gestion de la confidentialité et du consentement avec les responsables de la confidentialité et de la conformité, il peut parfois être tentant pour les RSSI de considérer le CIAM dans son ensemble comme un projet de marketing et de perdre tout intérêt par rapport à d'autres initiatives prioritaires. Les résultats de l'IAM traditionnel de la main-d'œuvre et de l'IAM grand public sont en effet assez différents, mais les deux bénéficieront de solutions commerciales qui stockent les données en toute sécurité et aident à atténuer le risque de violation de données – les identités des employés et des consommateurs méritent d'être protégées. De plus, si les initiatives CIAM se poursuivent sans tenir compte de manière stratégique de l'état actuel de l'infrastructure IAM, le RSSI peut se retrouver avec des fragments de solution fragmentaires supplémentaires dans l'environnement de son organisation, augmentant le risque avec des points d'accès supplémentaires. Il est dans l'intérêt du RSSI de regrouper les cas d'utilisation IAM de la main-d'œuvre et des consommateurs sous une seule solution lorsque cela est possible afin d'éviter les silos de données inutiles.

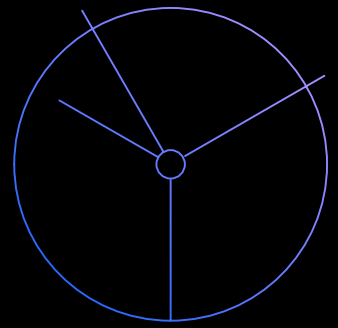


Chief Information Officers – (CIO)

Objectif CIAM : réduire les complexités de l'adoption et de la maintenance des solutions IAM tout en respectant les dernières normes d'identité pour maintenir une posture de sécurité moderne

Mis à part les avantages de l'engagement des consommateurs de CIAM, le CIO doit évaluer chaque nouvelle décision technologique pour qu'elle s'intègre dans l'infrastructure holistique et le plan opérationnel de l'organisation. La simplicité et la standardisation sont idéales, alors associer les fonctionnalités IAM et CIAM dans un seul outil devrait résonner auprès du leadership informatique tout comme avec la sécurité. Avec cette approche, l'environnement informatique global n'augmente pas en complexité et ne nécessite pas de nouvelles compétences de la part du personnel existant. Il y aura probablement un avantage financier à réutiliser la même solution pour les populations externes également, en maintenant les dépenses d'exploitation informatiques globales au minimum.

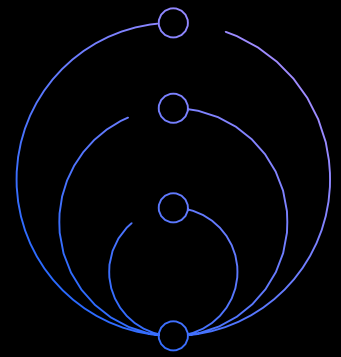
Une fois qu'une solution CIAM est opérationnelle, chaque minute d'indisponibilité peut entraîner une perte de temps et de revenus préjudiciable pour les organisations dont les clients ne peuvent pas accéder à leurs comptes. Rien que cela expliquerait pourquoi de nombreux responsables informatiques préfèrent les solutions basées sur le cloud pour les cas d'utilisation CIAM du point de vue du retour sur investissement, car elles ont tendance à offrir une disponibilité et une évolutivité beaucoup plus élevées que les alternatives sur site. Néanmoins, l'IAM cloud offre des incitations supplémentaires au personnel informatique, telles qu'une maintenance réduite de l'infrastructure, des mises à jour logicielles automatiques et un délai de rentabilisation plus rapide.



Administrateurs et développeurs IAM

Objectif CIAM : Simplifier le travail de développement et protéger et maintenir les politiques d'application grâce à des flux de travail low-code et basés sur la configuration

Alors que les parties prenantes exécutives s'alignent sur les objectifs commerciaux de niveau supérieur, les coûts d'exploitation et l'atténuation des risques, les administrateurs et les développeurs IAM peuvent influencer le développement du programme CIAM en évaluant les capacités techniques des solutions à tous les niveaux. Ils peuvent examiner la logistique pour la migration ou la fusion des sources de données et des applications, ainsi que des éléments clés tels que les protocoles d'authentification pris en charge, les méthodes MFA et les canaux de livraison. Pour accélérer la rentabilisation, cette équipe peut évaluer la documentation des API, les ressources guidées et les expériences low-code des solutions, ainsi que pour s'assurer que leur équipe sera bien prise en charge tout au long de la mise en œuvre et de la maintenance de la solution. Les fonctionnalités basées sur les flux de travail, telles que la gestion des consentements dans l'outil CIAM, peuvent éviter aux développeurs des maux de tête, par exemple en faisant abstraction des détails des lois sur la confidentialité en de simples appels d'API qui tiennent automatiquement compte de l'évolution des exigences. Avant qu'un autre outil ne soit ajouté au mélange, le personnel technique doit évaluer de manière globale la compatibilité et l'intégration avec leurs solutions IAM existantes pour garantir une adéquation optimale à long terme.



L'approche CIAM intégrée d'IBM

Modernisez les expériences numériques avec l'approche CIAM intégrée d'IBM

Avec IBM Security, votre organisation peut capturer et se connecter avec vos clients via des engagements omnicanaux à la demande, personnalisés et sécurisés en utilisant un mélange de stratégie d'identité, d'expertise en conception numérique et de technologie CIAM native du cloud. En utilisant IBM Security Verify associé à IBM Security Services, vous pouvez aider à établir un alignement organisationnel, suivre les informations des consommateurs avec respect et précision et ravir les consommateurs avec des expériences numériques simples et sécurisées de votre marque.

Étapes suivantes

Allez plus loin avec CIAM
En savoir plus sur les meilleures pratiques CIAM, les considérations de planification et les pièges à éviter

Télécharger le guide →

Explorez IBM Security Verify
Utilisez IDaaS pour moderniser les expériences utilisateur grâce à la connexion sociale et à l'authentification adaptative tout en préservant la confidentialité grâce à la gestion des consentements

En savoir plus sur Verify →

IBM Security CIAM Services
Planifier, concevoir, déployer et exécuter un programme CIAM par rapport aux objectifs commerciaux en utilisant une approche consultative et collaborative unique

Obtenir de l'aide avec CIAM →

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique
Février 2021

[1] Marchés et marchés, prévisions mondiales du marché IAM grand public jusqu'en 2025