



ÉTUDE
(C)IAM
2022

LES PRINCIPAUX
RÉSULTATS

présentés par



auth0

okta

CIAM – S’orienter davantage vers le client



Eugenio Pace,
PDG Auth0

Les Allemands portent le costume folklorique tyrolien (culottes de cuir et dirndl), ils n’ont pas beaucoup d’humour, un penchant pour la bière et les voitures et sont tous très travailleurs. Un pur cliché. Mais est-ce que ces caractéristiques reflètent vraiment l’identité allemande ? Il n’est possible de l’affirmer que lorsque l’on sait qu’une personne est vraiment celle qu’elle prétend être. Les spécialistes parlent en la matière de gestion des identités et des accès clients, en anglais « Customer Identity and Access Management », ou CIAM en abrégé.

Auth0 a demandé à IDG de réaliser une étude de tendance pour savoir comment les responsables de l’informatique et de la sécurité voient exactement la gestion de ces diverses identités de clients au sein de leur entreprise. Qu’est-ce qui est pertinent à leur avis aujourd’hui et à l’avenir, quelles mesures doit-il en découler selon eux pour mettre en place un CIAM efficace ? Et avec qui est-il urgent de travailler sur ce sujet ?

L’étude vous apporte des informations concrètes sur ce que doivent être vos cas d’utilisation (Use Cases) de gestion

des identités, afin de disposer des bases nécessaires pour réussir votre stratégie CIAM. Vous apprendrez également à quel moment les systèmes IAM atteignent leurs limites et, enfin et surtout, qu’il est important de rechercher un partenariat avec les développeurs de logiciels, les gestionnaires des produits et le marketing numérique.

Auth0 souhaite vous apporter à travers cette étude un guide solide qui vous donne les facteurs clés de réussite pour distinguer clairement l’organisation des identités des salariés de la gestion des identités numériques des clients. Et aussi vous permettre de comprendre comment un système CIAM peut facilement être mis en place à partir d’un IAM.

Je peux dès maintenant vous dévoiler que certains résultats n’auront rien de surprenant pour vous, tandis que d’autres vous étonneront. Dans tous les cas, il est conseillé de modifier son point de vue et de miser sur un partenariat interdisciplinaire.

Je vous souhaite une bonne lecture.

Le client est souvent négligé

Pour 69 %* des entreprises interrogées, les critères de stratégie cités pour le CIAM sont les infrastructures et la sécurité informatiques. Par contre, seulement 22 % d'entre elles ne tiennent compte dans leur stratégie CIAM d'un accès client unique en cas d'utilisation de plusieurs services. 19 % prévoient la possibilité d'une authentification par les réseaux sociaux, ou « social login », pour le compte client.

Alors que 33 % des services spécialisés considèrent qu'une connexion unique des clients pour plusieurs services doit faire partie de la stratégie CIAM, seules 21 % des personnes interrogées dans le domaine informatique le pensent, et seulement 11 % aux niveaux de la direction d'entreprise et du comité directeur.

Manifestement, les critères qui dominent sont ceux qui sont également pertinents dans une stratégie IAM classique, comme l'authentification, l'inscription, la conformité, la protection des données et la gestion des risques, qui reste toujours un critère important pour 49 % des personnes interrogées.

Les exigences spécifiquement liées à la fidélisation des clients, au parcours des clients, à une expérience uniforme pour toutes les marques, à

un accès client unique pour l'utilisation de plusieurs services et à l'automatisation du marketing, sont citées au maximum à 29 %.

Cela semble indiquer que la majorité des entreprises interrogées tentent de mettre en œuvre la CIAM à partir de leur stratégie IAM existante. Dans de nombreuses entreprises, la stratégie IAM dépend cependant du service informatique et non pas des services spécialisés comme le développement ou le marketing, alors que c'est justement le marketing qui doit s'occuper de la mise en œuvre du parcours client.

Afin que l'aspect Client prenne une place plus importante dans la stratégie CIAM, il semble judicieux d'impliquer d'autres domaines de l'entreprise en plus du service informatique.

Quels sont les critères retenus dans votre stratégie CIAM ?

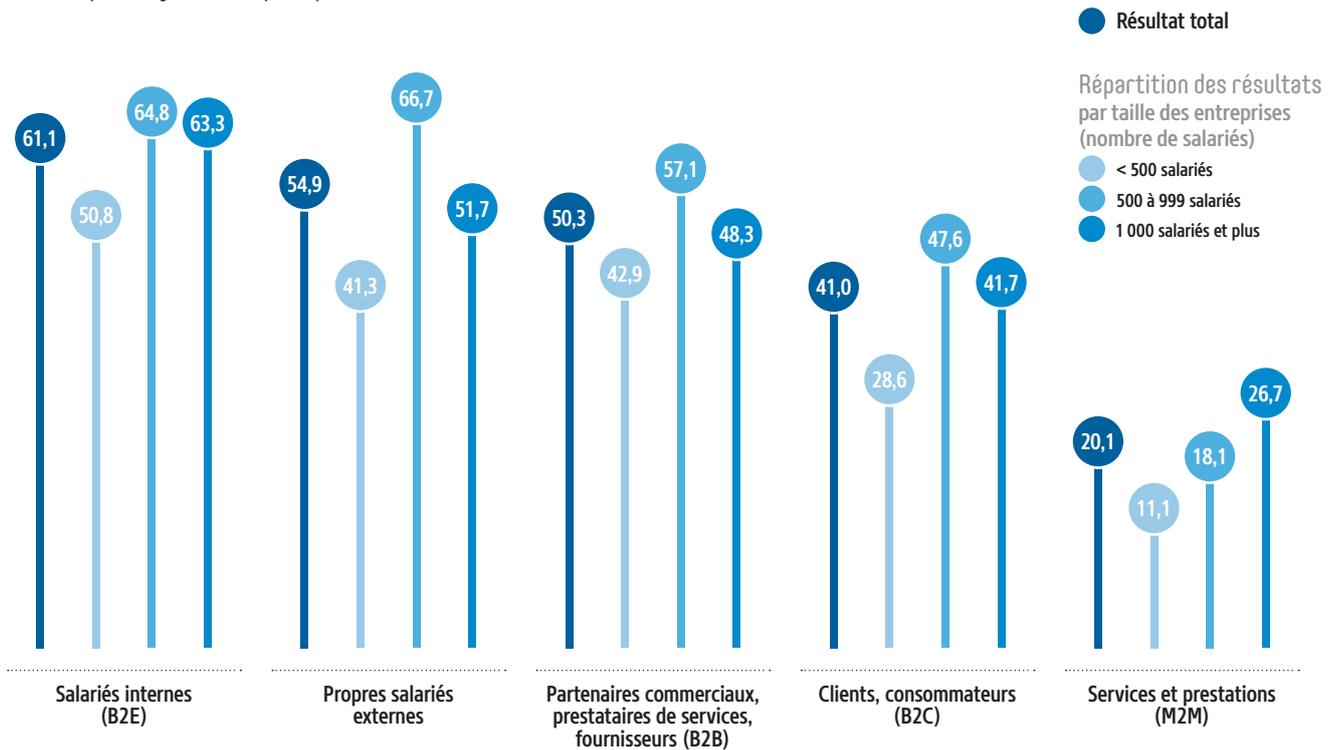
Données en pourcentage. Plusieurs réponses possibles. Filtre : Entreprises dans lesquelles il existe une stratégie CIAM spécifique. Base : n = 184

* Afin de répondre aux exigences d'une étude valide, un total de 288 entretiens qualifiés ont été menés auprès de responsables (informatiques) d'entreprises de la région DACH issus de toutes les divisions de l'entreprise (niveau C, informatique, départements spécialisés) et de tous les secteurs.

Infrastructure informatique (authentification, inscription)	68,5
Sécurité informatique (conformité, protection des données)	68,5
Gestion des risques	48,4
Calendrier de la mise en œuvre de la gestion CIAM	44,0
Validation du login	35,3
Données centralisées	34,8
Utilisation des identités clients conforme à la loi	33,2
Marketing (fidélisation clients / parcours client)	28,8
Expérience uniforme pour toutes les marques	25,5
Accès client unique pour l'utilisation de plusieurs services	21,7
Automatisation du marketing (social login pour le compte client)	18,5

Qui (ou quoi) accède aux systèmes de votre entreprise par le biais d'outils d'authentification et de gestion de l'identité ?

Données en pourcentage. Plusieurs réponses possibles. Base : n = 288



Dans le secteur du commerce de détail, les besoins en gestion IAM augmentent

La plupart du temps, ce sont les salariés de l'entreprise qui accèdent à ses systèmes informatiques par le biais d'outils de gestion des identités (61 % d'accès internes, 55 % d'accès externes) ou les partenaires et fournisseurs (50 %). Dans 41 % des entreprises, ces accès proviennent déjà de clients.

Les entreprises qui ont opté pour un accès client via un système IAM, font toutes état de ce type d'utilisation. Mais aussi les collaborateurs internes, les partenaires et les fournisseurs ainsi que des machines accèdent de plus en plus souvent aux systèmes de ces entreprises via des solutions IAM / CIAM. Ainsi, les utilisateurs de CIAM font état à 64 % d'accès internes et externes des collaborateurs, à 57 % d'accès de partenaires et à 28 % d'accès M2M par le biais de solutions IAM.

Les entreprises comptant entre 500 et 999 salariés indiquent une fréquence des accès des clients finaux de 48 %, contre 29 % seulement pour les entreprises de moins de 500 salariés et 42 % pour les entreprises de plus de 1 000 salariés.

Le budget informatique annuel a également une influence sur la fréquence à laquelle les clients accèdent à l'informatique de l'entreprise via une solution de gestion des identités. Si 38 % des entreprises qui disposent d'un budget informatique inférieur à dix millions d'euros par an font état d'accès clients, cette proportion passe à 46 % pour les budgets informatiques annuels supérieurs à 10 millions d'euros.

Il convient de tenir compte du fait que l'accès interne aux systèmes IAM est différent des accès externes par les utilisateurs finaux, car ceux-ci peuvent utiliser des plateformes et des périphériques très différents et leurs identifiants (mail) changent plus souvent.

3

Ce sont principalement les données clients qui sont traitées par l'outil IAM

Dans 70 % des entreprises, les solutions IAM traitent des données clients, dans 63 % des cas des données des salariés et dans 58 % des cas des données de partenaires. Les données commerciales et contractuelles sont citées à 58 % et les données machines et capteurs à 25 %. Dans le cas des entreprises où les clients accèdent via une solution IAM, elles sont même 83 % à traiter les données des clients dans la gestion des identités.

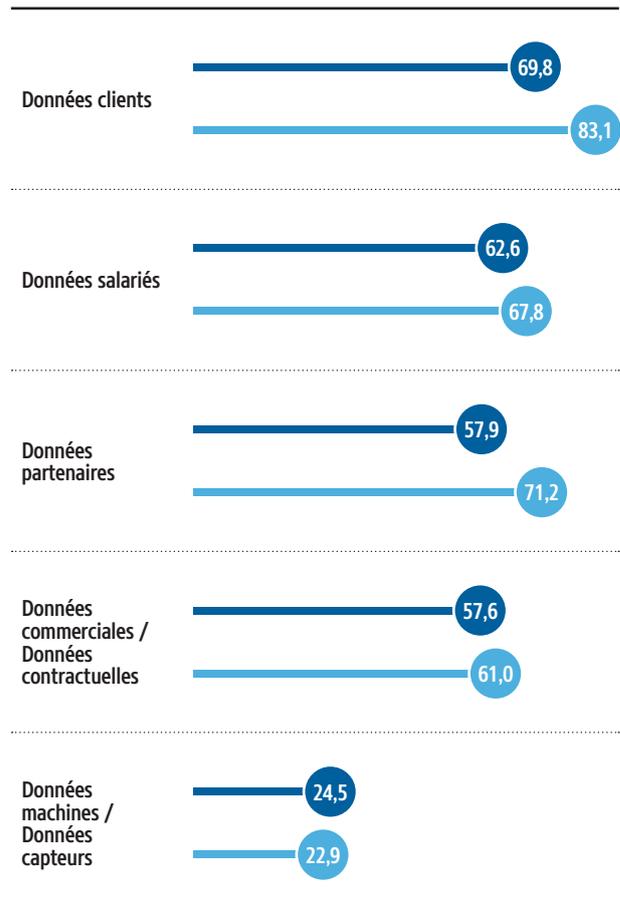
Les données clients dominent le traitement des données dans un système IAM, même si l'on ne considère pas uniquement les entreprises qui autorisent les accès clients à leur IAM.

En particulier dans les entreprises entre 500 et 999 salariés, 75 % traitent les données clients dans des systèmes IAM. Dans le cas des plus grandes entreprises, comptant au moins 1 000 salariés, ce pourcentage tombe à 66 %, et à 68 % dans les entreprises plus petites avec moins de 500 salariés.

Le budget informatique disponible pour l'année a également une certaine influence sur l'étendue du traitement des données client dans un système IAM. Un budget informatique relativement bas ne signifie pas forcément que les données clients sont traitées moins souvent dans l'IAM, bien au contraire. Dans les entreprises qui disposent d'un budget informatique inférieur ou égal à dix millions d'euros, 71 % d'entre elles traitent les données client dans l'IAM. Lorsque ce budget est plus important, ce pourcentage tombe à 69.

Quels types de données sont traités dans votre entreprise au moyen des services d'IAM ?

Données en pourcentage. Plusieurs réponses possibles.



- Entreprises dans lesquelles une gestion des accès et des identités (IAM) est effectuée sur site ou dans le cloud. Base : n = 278
- Filtre : Entreprises dans le cas desquelles les clients et / ou les consommateurs (B2C) accèdent à des systèmes de l'entreprise par des outils d'authentification et de gestion des identités. Base : n = 118

Il est donc possible d'en conclure qu'il existe un grand potentiel pour la gestion CIAM dans la grande majorité des entreprises, car elles gèrent déjà des données clients dans leur système IAM.

4 Le service informatique et le service sécurité dominant la stratégie CIAM

84 % des entreprises citent le service informatique comme instance décisionnaire de la stratégie CIAM, 57 % indiquent la sécurité informatique. Par contre, 44 % seulement citent le service développement, lequel pourrait par exemple apporter dans la stratégie de nouvelles fonctions d'authentification des clients, 42 % citent le service clients et 16 % citent le service juridique.

Les entreprises qui comptent moins de 500 salariés citent particulièrement souvent (89 %) le service informatique comme décideur dans la stratégie CIAM. Dans les entreprises comptant entre 500 et à 999 salariés, le pourcentage de personnes qui pensent que le service informatique est décisif pour le CIAM tombe à 82 %, et à 84 % pour les entreprises de 1 000 salariés et plus.

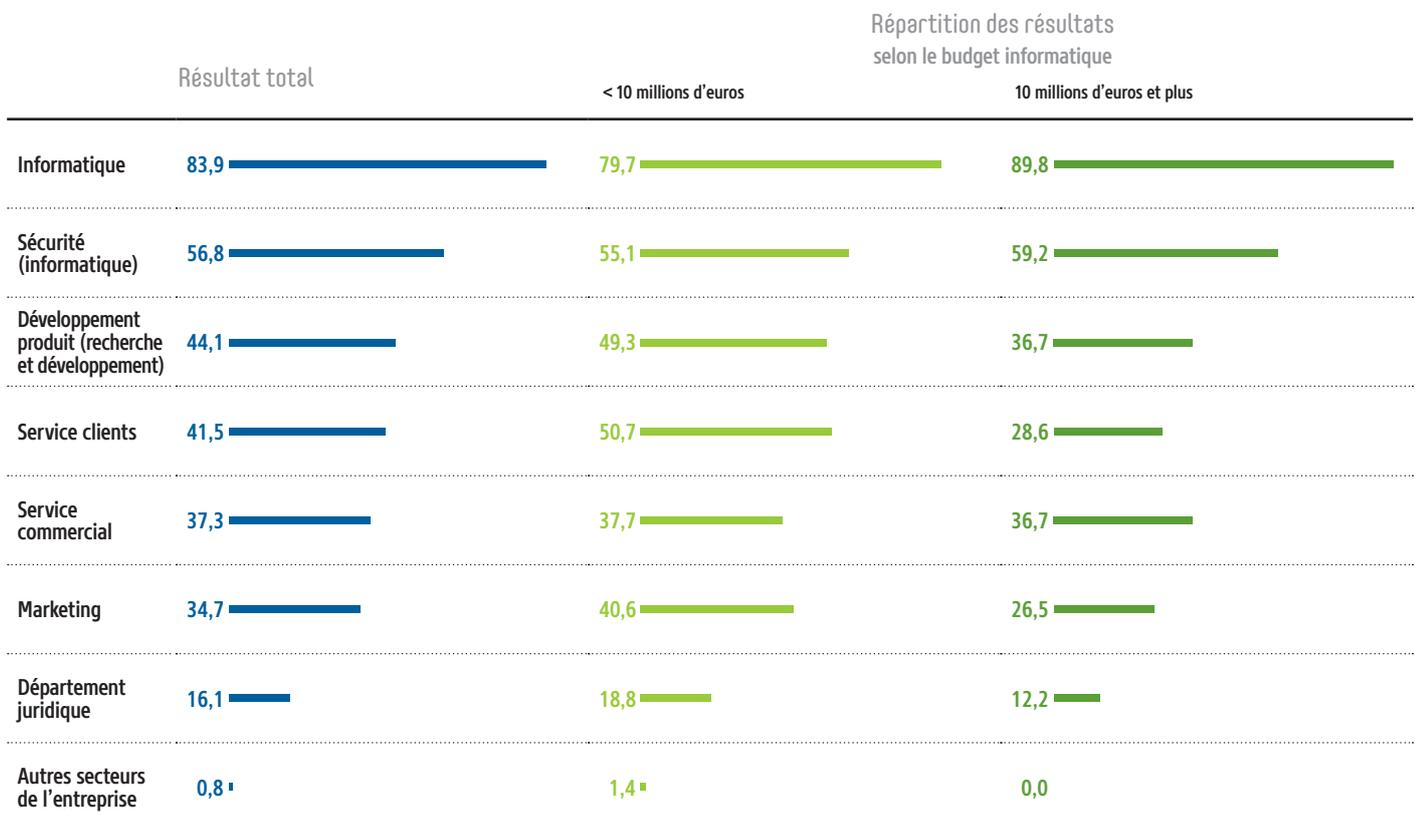
Cependant, la sécurité informatique est particulièrement peu citée par les entreprises de moins

de 500 salariés, seulement à 33 %, contre 68 % dans le cas des entreprises de 500 à 999 salariés et 54 % à partir de 1 000 salariés.

En revanche, le service développement est plus important pour les petites entreprises que pour les grandes. Le nombre d'entreprises qui considèrent le service développement comme un service décisif pour la gestion CIAM est de 61 % pour les entreprises de moins de 500 salariés, de 48 % pour les entreprises de 500 à 999 salariés et de 34 % à partir de 1 000 salariés.

Quels sont les services de l'entreprise impliqués dans les processus décisionnels concernant la stratégie CIAM ?

Données en pourcentage. Plusieurs réponses possibles. Filtre : Entreprises dans le cas desquelles les clients et/ou les consommateurs (B2C) accèdent à des systèmes de l'entreprise par des outils d'authentification et de gestion des identités. Base : n = 118



4

.....▶ Si l'on compare l'importance accordée au domaine informatique et à la sécurité informatique en matière de gestion CIAM avec les critères que les entreprises citent pour la stratégie CIAM, tout se recoupe. Ici aussi, les critères concernant les clients ne sont pas la priorité.

Le poids important accordé au service informatique et à la sécurité informatique en tant que décideurs dans la stratégie CIAM peut entraîner le lancement de projets CIAM à partir d'un projet IAM existant, car le service informatique est déjà fortement impliquée dans l'IAM. Les solutions IAM classiques seraient ainsi utilisées pour des projets CIAM, sans toutefois pouvoir offrir les fonctions nécessaires dont le CIAM a besoin. L'assistance de multiples plateformes et périphériques que

les clients peuvent utiliser en fait notamment partie. Les services en contact avec les clients et le service développement sont à ce jour moins présents dans les décisions CIAM, ce qui peut entraîner une intégration insuffisante des nouvelles fonctions et priorités clients dans les stratégies CIAM.

C'est pourquoi il est recommandé de continuer à accorder une grande importance au service informatique et à la sécurité informatique dans les projets CIAM, mais aussi d'impliquer davantage dans les décisions le service développement et les services qui concernent directement les clients. Cela garantira par exemple de mieux tenir compte dans la stratégie CIAM des processus d'authentification modernes souhaités par les clients, sans avoir à faire des compromis sur la sécurité.

Quels sont les services de l'entreprise impliqués dans les processus décisionnels concernant la stratégie CIAM ?

Données en pourcentage. Plusieurs réponses possibles. Filtre : Entreprises dans le cas desquelles les clients et/ou les consommateurs (B2C) accèdent à des systèmes de l'entreprise par des outils d'authentification et de gestion des identités. Base : n = 118

Répartition des résultats
par taille des entreprises (nombre de salariés)





Auth0
un pôle de produits au sein d'Okta
<https://auth0.com/fr>

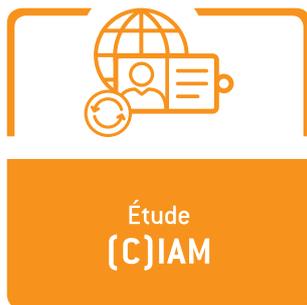
Historique de notre partenaire d'étude

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>.

Ce qui différencie IAM et CIAM

	CIAM	IAM
Adaptabilité	Les systèmes CIAM doivent être capables de gérer des flux de données considérables et de les adapter pour des millions de clients.	Les systèmes IAM doivent adapter les flux de données pour des centaines de salariés.
Sécurité	Les entreprises ne connaissent pas les clients qui accèdent aux services. La protection des données de l'entreprise ne peut fonctionner qu'au moyen de la connexion avec identifiants.	Les salariés qui accèdent aux services sont connus des entreprises. Il existe plusieurs options de protection, puisque les connexions sont effectuées par différents accès.
Disponibilité	La gestion CIAM nécessite un service cloud avec une redondance élevée. En effet, si les clients ne peuvent pas accéder aux services ou si les portails en ligne tombent en panne, l'entreprise perd du chiffre d'affaires.	Les systèmes IAM devraient également être délocalisés sur le cloud. L'impossibilité pour les employés d'accéder aux services nuit à la productivité et à la satisfaction au travail.
Flexibilité	Les cas d'utilisation des clients finaux sont plus variés et exigent donc plus de flexibilité selon le scénario. En effet, les clients peuvent accéder à un service à partir de n'importe quel périphérique, et ils disposent de possibilités de connexion individuelles, par exemple avec un nom d'utilisateur et un mot de passe ou par un profil de réseaux sociaux. Ces derniers doivent éventuellement être associés en arrière-plan afin que l'utilisateur puisse profiter d'un accès centralisé.	Les employés utiliseront des appareils appartenant à l'entreprise ou des appareils personnels sur lesquels seront installées les politiques de l'entreprise relatives aux appareils. Ils doivent pouvoir s'authentifier rapidement et en toute sécurité auprès de plusieurs applications professionnelles.



Mentions légales

Conception de l'étude / développement du questionnaire :
Simon Hülsbömer, Matthias Teichmann

Rédaction finale / CvD Volume du rapport d'étude :
Simon Hülsbömer

Analyses / commentaires : Oliver Schonschek

Hébergement / coordination du travail sur le terrain : Armin Rozsa

Direction artistique & graphisme : Daniela Petrini, Reutte

Conception de la couverture avec une photo couleur de © shutterstock.com/LuckyStep

Relecture : Elke Reinhold, Munich

Éditeur :

IDG Tech Media GmbH

Georg-Brauchle-Ring 23
80992 München, Allemagne
Téléphone : +49 89 36086-0
Mail : info@idg.de

Représentant autorisé : Jonas Triebel, gérant

Registre du commerce de Munich : HRB 99110,
N° TVA communautaire DE 811257834

Plus d'informations sur : www.idg.de