ForgeRock®

Comment évaluer les fonctionnalités stratégiques des solutions de CIAM

Caractéristiques essentielles, définitions et questions à poser aux fournisseurs

Table des matières

Les huit tendances qui façonnent la transformation digitale des entreprises

Huit tendances redessinent activement et de manière interdépendante la transformation digitale des entreprises et de la société, ajoutant de la complexité au paysage dans lequel les entreprises doivent évoluer. Pour survivre et prospérer à l'ère post-pandémique, les organisations doivent être équipées pour faire face à chacune d'elles.

1. Disruption. L'économie de la réinvention
La pandémie a tout bouleversé. Les entreprises doivent se réinventer afin d'acquérir et d'engager leurs clients, d'atténuer leurs pertes et d'assurer l'avenir de leur activité.

2. Écosystèmes partenaires
Dans le cadre de leur réinvention, les entreprises se lancent dans des écosystèmes numériques multipartites pour répondre à la demande insatiable des consommateurs en matière d'expériences exceptionnelles et de commodité.

3. Expériences phygitales
Quel que soit le mode ou l'endroit où les consommateurs interagissent avec une organisation, ils veulent une expérience transparente qui allie les éléments physiques et numériques.

4. Appareils intelligents et Internet des objets (IoT)
En grande partie en réponse aux demandes phygitales, le marché mondial de l'IoT grand public devrait passer de 97,50 milliards de dollars en 2020 à un montant estimé à 188,34 milliards de dollars en 2026.[1] Malheureusement, la plupart des « objets » ne sont pas sécurisés.

5. Cybercriminalité, violations, fraudes et excès
Le nombre de violations de données, de fraudes, de ransomwares et autres cybercrimes est monté en flèche, sans aucun signe de ralentissement.

6. Opinion publique et militantisme
Nous vivons aujourd'hui à l'ère de la méfiance. L'opinion publique offre un visage défensif. Les consommateurs veulent contrôler leurs données personnelles et veulent que les entreprises soient responsables de leurs actes et de leur gestion.

7. Vie privée, consentement et réglementation des données
En réponse à la demande du public, les gouvernements du monde entier ont adopté des réglementations concernant la vie privée, le consentement et les données. On s'attend à des évolutions dans les années à venir.

8. Générations Z, Alpha et le métavers
La génération Z est aujourd'hui la plus nombreuse, constituant 32 % de la population mondiale.[2] Derrière eux, la génération Alpha a moins de 12 ans, mais ses membres influencent déjà les achats à hauteur de plus de 500 milliards de dollars. Dans les années à venir, les générations Z et Alpha ne se contenteront pas de jouer dans le métavers, elles y travailleront, y feront des achats et y investiront !

Pour en savoir plus sur ces huit tendances, téléchargez ce document : **Les 8 tendances qui façonnent la transformation des entreprises et de la société.**

1 https://www.marketdataforecast.com/market-reports/consumer-iot-market
2 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/

Les huit tendances de la transformation digitale

> **Il est essentiel de se doter des capacités nécessaires pour l'avenir, et notamment pour créer une entreprise résiliente, capable de percevoir la volatilité et la disruption et d'y répondre.[3]**
>
> Gartner

Ces huit tendances de la transformation digitale constituent une force dominante. Elles nécessitent que les entreprises soient à même de :

- réinventer leurs stratégies commerciale et informatique pour faire face à tout type de perturbation et répondre aux demandes des consommateurs avec agilité et résilience en fonction du besoin,
- participer en toute sécurité à des écosystèmes numériques multipartites,
- offrir à leurs clients des expériences sécurisées et fluides sur tous les canaux de vente physiques et numériques,
- sécuriser l'IoT et gérer les relations entre les personnes et les appareils connectés,
- respecter les réglementations relatives à la vie privée, au consentement et aux données et s'imposer comme étant dignes de confiance,
- identifier les risques et se protéger contre la cybercriminalité et la fraude,
- préparer l'avenir de leur activité pour répondre à la demandes des générations qui arrivent sur le marché.

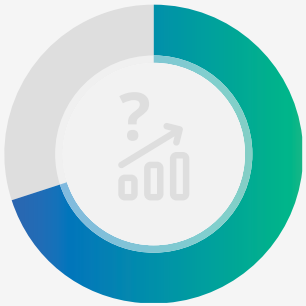
Malheureusement, ces exigences représentent souvent de véritables défis pour les entreprises aujourd'hui.

3 Gartner, The C-Suite Guide: Accelerate Digital for Future-Ready Business. Frameworks for composable tech, empowered customers and the future of work, 2021

L'échec des systèmes traditionnels et disparates

Dans le contexte de ces tendances, les entreprises cherchent à acquérir des clients plus rapidement et à leur offrir une expérience exceptionnelle, tout en se conformant aux réglementations et en assurant à la fois la sécurité de leurs clients et celle de l'entreprise. Pourtant, les écosystèmes informatiques traditionnels rendent souvent cet objectif difficile à atteindre.

70 % des répondants jugent la croissance disruptive essentielle à la réussite de leur entreprise, cependant seulement 13% d'entre eux pensent qu'elle peut répondre à cette priorité stratégique.[4]



Deloitte.

Par conséquent, la première étape vers la réinvention, consiste à effectuer l'inventaire des systèmes et processus existants utilisés dans leur entreprise.

Systèmes multiples et silos

Pour collecter, sécuriser et gérer les identités et les données des clients, des partenaires et de l'IoT, la plupart des entreprises utilisent encore une multitude de systèmes disparates à travers différents services.

BMW a fait appel à ForgeRock pour consolider 20 systèmes différents de gestion des identités et des accès en une seule plateforme ce qui a permis de réaliser d'importantes économies, d'améliorer les délais de mise sur le marché, la capacité d'évolution et la conformité.[5]

Par exemple, un service marketing peut utiliser une multitude de solutions logicielles pour collecter des données concernant les clients, telles que la géolocalisation et l'historique des achats. Dans le même temps, le service informatique peut utiliser un patchwork de systèmes distincts pour gérer la sécurité de solutions spécifiques ainsi que les données qu'elles recueillent, et bien sûr de l'entreprise dans son ensemble.

Les multiples systèmes engendrent des silos et une multitude de conséquences indésirables. Par exemple, non seulement les systèmes disparates empêchent une vision unifiée et exacte sur les clients, mais ils rendent l'évaluation des risques plus difficile, augmentant ainsi la probabilité de non-conformité réglementaire. En outre, plus il y a de points d'accès au sein d'une organisation, plus le risque de faille est élevé.

4 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf
5 https://www.forgerock.com/resources/view/108814636/customer-story/bmw-motors-into-the-digital-era-with-forgerock.pdf

Gestion des identités et des accès traditionnels

Dans un effort de réduction des coûts, de nombreuses entreprises ont tenté de modifier leurs systèmes de gestion des identités et des accès collaborateurs (IAM) existants pour répondre aux tendances et aux demandes, plutôt que d'investir dans une plateforme CIAM d'entreprise, conçue spécifiquement pour les utilisateurs externes. Pourtant, comme l'ont démontré les perturbations liées à la pandémie, les résultats sont loin d'être idéaux.

Tenter d'adapter des systèmes IAM existants qui n'ont pas la flexibilité, l'extensibilité ou l'évolutivité requises est un piège commun aux entreprises...[6]

ComputerWeekly

Les systèmes IAM existants sont développés pour prendre en charge les cas d'utilisation des collaborateurs ; ils ne sont pas conçus pour sécuriser et gérer des millions ou des milliards d'identités de clients, de partenaires et d'objets connectés - sans parler de leurs données. De même, l'IAM existant n'est pas conçu pour offrir des expériences multicanales fluides, ni pour prendre en charge les réglementations relatives à la confidentialité et aux données tel que le Règlement Général sur la Protection des Données (RGPD), ni pour atténuer le risque de cybercriminalité et de fraudes. De plus, ces solutions IAM ne prennent pas en charge les normes modernes, ce qui les empêche de répondre aux cas d'utilisation intermédiaires à avancés des clients, des partenaires et de l'IoT aujourd'hui. Il est également très difficile et coûteux de les mettre à niveau... Pourtant, elles doivent être mises à niveau pour répondre aux cas d'utilisation les plus élémentaires, sans parler des tendances et des attentes actuelles.

6 https://www.computerweekly.com/news/450429018/Consumer-identity-management-will-benefit-business

Solutions d'IAM traditionnelles dans le cloud

Pour tenter d'obtenir rapidement et facilement la fonctionnalité CIAM dont elles avaient besoin, de nombreuses entreprises ont implémenté des solutions IAM traditionnelles dans le cloud. Ces toutes premières solutions d'IAM dans le cloud se concentraient principalement sur la simplicité pour les petites et moyennes entreprises, au détriment des fonctionnalités et de la flexibilité nécessaires aux plus grandes organisations.

98 %

des early adopters de solutions d'IAM (cloud-only) ont cité des défis.[7]

FORRESTER®

Les grandes entreprises ont besoin de fonctionnalités plus étendues que celles que les solutions traditionnelles d'IAM dans le cloud peuvent offrir. Il s'agit notamment de la sécurité et de la flexibilité qui sont incontournables dans l'entreprise.

Dans une étude réalisée par Forrester en 2021, la quasi-totalité (98 %) des primo adoptants des solutions traditionnelles de gestion des identités et des accès (IAM) dans le cloud ont fait état de difficultés, et notamment :

- L'absence d'intégration aux processus existants
- L'incapacité à gérer les identités à travers les applications et systèmes actuels
- Manque de visibilité sur les systèmes sur site, d'où une vision incomplète des risques et du niveau de sécurité.

L'obstacle le plus récurrent auquel sont confrontées les personnes interrogées par Forrester est l'incapacité à mettre en correspondance ou à intégrer les processus ou les solutions existants. Les processus métiers et les intégrations des identités varient considérablement d'une application à l'autre. Chacune prend en charge des normes et des protocoles différents. Cela rend complexe toute solution d'IAM dans le cloud qui ne prend pas en charge les normes requises ou qui n'offre pas la flexibilité et l'extensibilité nécessaires pour s'adapter aux besoins des entreprises. En d'autres termes, ces solutions d'IAM traditionnelles dans le cloud ne peuvent pas s'intégrer de manière transparente aux applications existantes ou récentes, ni s'adapter aux processus métiers de l'entreprise.

7 https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam

La voie à suivre : le CIAM d'entreprise

Contrairement aux solutions d'IAM traditionnelles dans le cloud, le CIAM (gestion des identités et des accès clients) est le fondement de la réinvention, de la sécurité et de la disruption. Les grandes entreprises l'utilisent pour répondre à chacune des huit tendances citées plus haut, tout en réduisant la charge pesant sur les ressources informatiques. Grâce au CIAM, elles acquièrent des clients plus rapidement, offrent des expériences exceptionnelles et protègent leurs clients ainsi que leur organisation en :

- réinventant leurs stratégies commerciale et informatique pour faire face à tout type de disruption et répondre aux attentes des clients avec agilité et résilience,
- participant en toute sécurité à des écosystèmes numériques multipartites,
- en offrant à leurs clients des expériences sécurisées et fluides sur tous les canaux de vente physiques et numériques,
- en sécurisant l'IoT et en gérant les relations entre les personnes et les appareils connectés,
- en respectant les réglementations relatives à la vie privée, au consentement et aux données et en s'imposant comme entreprise de confiance,
- en identifiant les risques et en se protégeant contre la cybercriminalité et la fraude,
- en préparant l'avenir de leur activité pour répondre aux attentes des générations qui arrivent sur le marché.

Le CIAM joue un rôle important dans la transformation digitale des entreprises aujourd'hui pour acquérir et fidéliser les clients, tout en leur fournissant les éléments de sécurité et de personnalisation nécessaires pour qu'ils s'engagent et effectuent des transactions en confiance avec l'entreprise.[8]

FORRESTER®

8 https://www.forrester.com/report/now-tech-customer-identity-and-access-management-ciam-q2-2020/RES160459?objectid=RES160459

Comment évaluer les fonctionnalités stratégiques des solutions de CIAM

Le tableau suivant énumère en détails les fonctionnalités et attributs essentiels des solutions de CIAM ainsi que les questions à poser aux fournisseurs de ces solutions dans le cadre d'un RFP. Les informations sont regroupées par catégories : basique, intermédiaire et avancé, qui reflètent la complexité des cas d'utilisation. La plupart des grandes entreprises auront des exigences avancées.

Fonctionnalités basiques

FONCTIONNALITÉS BASIQUES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
SSO fédéré	Basée sur des relations de confiance « fédérées » entre les entreprises, l'authentification unique (SSO) fédérée permet aux utilisateurs, tels que les partenaires, d'accéder en toute sécurité aux propriétés et applications web de l'entreprise à l'aide d'un compte unique, d'où l'authentification unique. Le SSO fédéré utilise des normes ouvertes telles que OAuth, WS-Federation, WS-Trust, OpenID Connect et SAML pour transmettre des jetons d'authentification entre les fournisseurs d'identité des entreprises. Cette capacité est utilisée pour offrir de meilleures expériences. Elle répond à la tendance liée aux écosystèmes de partenaires et à la cybercriminalité.	• Le fournisseur offre-t-il une authentification unique fédérée reposant sur des normes ouvertes telles que OAuth, WS-Federation, WS-Trust, OIDC et SAML ?
Inscription et authentification sociale	En tant que forme d'authentification unique (SSO), l'inscription et l'authentification sociales permettent aux utilisateurs de s'inscrire et de s'authentifier rapidement et facilement en utilisant leurs informations existantes à partir d'un service de réseau social, tel que Google ou Facebook par exemple. Cette capacité est utilisée pour offrir de meilleures expériences. Elle répond aux tendances liées à l'expérience phygitale, à la génération Z et la génération Alpha, ainsi qu'à la cybercriminalité.	• Le fournisseur propose-t-il l'inscription et l'authentification via les réseaux sociaux ? • Lesquels sont inclus dans leur offre ? • Comment l'administrateur de la solution CIAM configure-t-il la vérification de l'identité sociale ?

FONCTIONNALITÉS BASIQUES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Authentification multifacteur (MFA)	L'authentification multifacteur (MFA) est une méthode de validation de l'identité d'un utilisateur par le biais de mécanismes d'authentification multiples. Les mécanismes d'authentification comprennent ce que l'utilisateur sait, ce qu'il possède et ce qu'il est. Par exemple, l'accès n'est accordé qu'après qu'un utilisateur a saisi son mot de passe (ce que l'utilisateur sait) et un code numérique envoyé par SMS sur son téléphone (ce que l'utilisateur possède). Cette capacité est utilisée pour protéger les clients et l'entreprise. Elle répond aux tendances liées à la cybercriminalité et à l'opinion publique.	• Le fournisseur propose-t-il une authentification multifactorielle ? • Quels mécanismes d'authentification offre-t-il ?
Autorisation	Dans le cadre du contrôle d'accès au cœur d'une solution de gestion des identités numériques, l'autorisation est la fonction qui consiste à déterminer si un utilisateur a la permission d'accéder à une ou plusieurs ressources spécifiques, telles qu'un ou plusieurs sites Web, un ou plusieurs dossiers, un ou plusieurs documents, etc. Cette capacité est utilisée pour protéger les clients et l'entreprise. Elle répond aux tendances liées aux écosystèmes de partenaires, aux expériences phygitales, à la cybercriminalité, à l'opinion publique et à la réglementation des données personnelles.	• Quels types de méthodes d'autorisation et de contrôles d'accès sont proposés par le fournisseur ?
Identity store	Dans le cadre des services d'annuaire, un identity store ou magasin d'identités est un référentiel pour les données d'attribution des identités. Les données d'identité stockées doivent être chiffrées tant au repos qu'en transit. De plus, les meilleures pratiques imposent d'avoir un référentiel intégrable qui peut facilement partager en temps réel les données d'identité des clients, des appareils et des utilisateurs sur plusieurs environnements. Du point de vue de l'hébergement, les identity stores doivent offrir une haute disponibilité, des performances et une sécurité élevées. Enfin, ils doivent être entièrement conformes à la norme LDAP v3 et s'intégrer de manière transparente à tout annuaire. Cet attribut est utilisé pour répondre aux tendances liées à l'économie de réinvention, aux écosystèmes de partenaires, aux expériences phygitales, à l'IoT, à la cybercriminalité et à la réglementation en matière de confidentialité de données.	• L'identity store de la solution chiffre-t-il les données à tout moment ? • La solution offre-t-elle une réplication fractionnée et multi-maîtres ? • Comment l'identity store évolue-t-il pour prendre en charge des données provenant de centaines ou de millions d'identités, y compris d'appareils et d'objets ? • L'identity store de la solution est-il conforme à LDAP v3 et s'intègre-t-il de manière transparente à n'importe quel annuaire ?

FONCTIONNALITÉS BASIQUES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Plateforme CIAM en mode SaaS **(Software as a Service)**	La maintenance et la mise à niveau des solutions de gestion des identités sont complexes et demandent beaucoup de travail. Avec une plateforme CIAM complète fournie sous forme de logiciel en tant que service (SaaS), les entreprises peuvent tirer parti des dernières fonctionnalités sans avoir à assumer la responsabilité de l'hébergement, de la maintenance, des mises à niveau, etc. Le CIAM en mode SaaS permet également aux ressources informatiques de se concentrer sur d'autres initiatives importantes, comme l'innovation. Les préoccupations en matière de sécurité - notamment le partage et la souveraineté des données - sont l'une des principales raisons pour lesquelles de nombreuses grandes entreprises ont hésité à passer à une plateforme CIAM complète dans le cloud. En effet, de nombreux fournisseurs de SaaS regroupent plusieurs clients (« tenants ») sur une seule instance. Cette approche dépassée du multi-tenant entraîne un risque élevé car les activités d'une entreprise peuvent avoir un impact sur d'autres. C'est pourquoi la plateforme CIAM en mode SaaS idéale offre une isolation complète de l'entreprise afin que les données et les charges de travail ne soient jamais mêlées aux autres. L'isolation des tenants élimine également les défis courants liés à l'évolution et au stockage des données d'identité sensibles et réglementées dans le cloud. La plateforme CIAM en mode SaaS doit également assurer la souveraineté et la conformité des données, ainsi qu'une disponibilité maximale avec des sauvegardes individuelles. Elle doit également inclure une architecture haute disponibilité avec un basculement automatique pour répondre aux exigences strictes des accords de niveau de service (SLA), ainsi qu'une sauvegarde et une restauration spécifiques à l'entreprise. Les entreprises peuvent ainsi récupérer rapidement et efficacement après tout problème de corruption accidentelle ou malveillante des données. Ce modèle d'architecture cloud est utilisé pour acquérir des clients plus rapidement, offrir des expériences exceptionnelles et protéger les clients et l'entreprise. Il répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, à la cybersécurité, à l'opinion publique et aux réglementations sur la vie privée et les données.	• La solution CIAM en mode SaaS offre-t-elle une isolation complète de l'entreprise dans une architecture multi-tenant ? • Comment la solution CIAM assure-t-elle la souveraineté granulaire des données ? • Comment le fournisseur de CIAM assure-t-il la résidence des données d'identité, d'application et de sauvegarde ? • Quel est le SLA de disponibilité du fournisseur de CIAM pour la solution SaaS ? • Comment le fournisseur utilise-t-il les standards du marché pour concevoir l'architecture de sécurité des données de la solution ? • Quelles évaluations, audits, examens ou certifications de tiers ont été obtenus pour la solution ?

Fonctionnalités intermédiaires

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Self-Service	Le self-service consiste à permettre aux utilisateurs de gérer eux-mêmes leurs comptes plutôt que de s'en remettre au personnel du support dans l'entreprise. Parmi les exemples de self-service, citons la gestion des préférences de connexion, la gestion des mots de passe, la mise à jour des informations de contact, les demandes d'assistance, etc. Le self-service permet non seulement de réduire les coûts d'assistance, mais aussi d'améliorer l'expérience des utilisateurs et l'engagement des clients. Cette capacité est utilisée pour offrir de meilleures expériences. Elle répond aux tendances liées aux écosystèmes de partenaires, aux expériences phygitales et aux générations Z et Alpha.	• Quelles fonctionnalités de self-service le fournisseur prend-il en charge et comment ? • Comment la solution CIAM personnalise-t-elle et thématise-t-elle les parcours de self-service pour les différentes populations d'utilisateurs ?
Usurpation d'identité sécurisée	Les membres d'une entreprise, comme le personnel du service support, ont parfois besoin de se faire passer pour un utilisateur (dans le bon sens du terme) afin de prendre des mesures en son nom. La fonction d'usurpation d'identité sécurisée permet aux utilisateurs de céder, de manière consensuelle, le contrôle temporaire de leur compte à une autre personne pendant une période déterminée. L'extension des services numériques des clients à des tiers nécessite la prise en charge de l'échange de jetons OAuth 2.0. Cette capacité est utilisée pour offrir de meilleures expériences et pour protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, aux générations Z et Alpha, à la cybersécurité, à l'opinion publique, à la confidentialité et à la réglementation des données.	• La solution CIAM prend-elle en charge l'échange de jetons OAuth 2.0, incluant une CIBA (authentification backchannel initiée par le client) ? • Comment le fournisseur gère-t-il les cas d'utilisation de la délégation de l'utilisateur final et de l'usurpation d'identité sécurisée ?
Vue unique sur les identités	Une vue unique de l'identité d'un client à l'échelle de l'entreprise améliore la sécurité, le service, les initiatives marketing, etc. Pour que les plateformes CIAM prennent en charge une vue unique sur les identités, elles doivent pouvoir s'intégrer à d'autres systèmes et consolider de multiples silos de données clients afin de créer une vue unique sur une identité à l'échelle de l'organisation. Cette capacité est utilisée pour offrir de meilleures expériences et pour protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, aux générations Z et Alpha, ainsi qu'à la cybercriminalité.	• Comment la solution s'intègre-t-elle aux autres systèmes afin de consolider les silos de données d'identités pour créer une vue unique sur le client à l'échelle de l'entreprise ? • La solution peut-elle fournir une synchronisation bidirectionnelle en direct et un rapprochement des attributs d'identités entre les data stores ? • Comment l'administrateur de la solution CIAM configure-t-il la migration des clients d'une solution CIAM antérieure vers la solution CIAM du fournisseur ? Comment prend-il en charge la migration progressive ? • Comment l'administrateur de la solution CIAM importe-t-il les hachages de mots de passe existants ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Disponibilité et évolutivité	L'évolutivité, les performances et la disponibilité sont essentielles à une plateforme CIAM, car si la plateforme ne fonctionne plus, l'activité non plus. Il est important d'avoir un plan pour les pics de connexion des utilisateurs, des appareils et des objets qui doit être stocké dans une base de données, de même que pour les changements de fréquences et de durées des sessions simultanées et concomitantes. Les fournisseurs de CIAM doivent prendre en charge à la fois la disponibilité du service et la disponibilité de la session. La disponibilité du service garantit que les utilisateurs peuvent accéder à un site lorsqu'un serveur tombe en panne. La disponibilité des sessions préserve et maintient une session en cours si un serveur tombe en panne. Les fournisseurs de CIAM doivent également prendre en charge une variété de scénarios d'évolution. Cela inclut un nombre changeant (souvent des millions) d'utilisateurs, d'appareils et d'objets à stocker dans une base de données, ainsi que des fréquences et des durées variables de sessions simultanées. Il est important d'éviter la latence dans la décision d'accès de microservice à microservice (les flux est/ouest sont assez prolifiques) en plus de la prise en charge d'un protocole sans état utilisant des jetons de session JWT. La disponibilité et l'évolutivité ne font pas seulement partie de la plateforme CIAM elle-même, mais aussi de la manière dont elle est hébergée. Voir la section CIAM Software as a Service pour les détails relatifs au cloud. Ces capacités sont utilisées pour acquérir des clients plus rapidement et offrir de meilleures expériences. Elles répondent aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales et à l'IoT.	Lorsqu'il s'agit d'évaluer la plateforme CIAM elle-même, et non son hébergement, il faut tenir compte des éléments suivants : • Le fournisseur de CIAM propose-t-il une analyse comparative des performances pour les transactions par section, le chargement des données d'identité, la synchronisation des données d'identité ? Quel est l'impact si un grand nombre d'IdP (10, 100 ou 1000) est nécessaire ? • La solution CIAM peut-elle faire évoluer le service d'inscription, d'authentification et d'autorisation des identités de plusieurs ordres de grandeur pour répondre aux pics prévus, comme lors d'un événement très médiatisé, ou lors d'événements imprévus, comme la demande de contenu tendance ou les activités des médias sociaux ? • Le fournisseur d'identité (IdP) prend-il en charge la disponibilité des sessions, la disponibilité avec état et les protocoles sans état ? Le fournisseur prend-il en charge les serveurs redondants, les équilibreurs de charge, les déploiements HA avec une réplication multi-maître à n-voies ? La solution s'étend-elle horizontalement dans les environnements multi-tenant ?
Support des normes ouvertes	Les normes ouvertes sont des normes techniques établies et uniformes, utilisées par les développeurs. Chaque norme possède des capacités et des fonctionnalités spécifiques. La sécurité de l'identité repose sur les normes OAuth2, OpenID Connect et SAML. Au-delà de ces normes d'identité de base, les meilleurs fournisseurs intègrent des normes nécessaires telles que UMA 2.0, qui permet aux utilisateurs de partager en toute sécurité l'accès à leurs données personnelles avec un tiers. Parmi les autres normes avancées, citons OAuth 2.0 Proof-of-Possession, qui garantit que le présentateur d'un jeton au porteur est le propriétaire réel et original du jeton, et OAuth2 Device Flow, qui est conçu pour les appareils clients qui ont une interface utilisateur limitée. Cette capacité est utilisée pour acquérir des clients plus rapidement, offrir de meilleures expériences et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, aux générations Z et Alpha, à la cybercriminalité et aux réglementations sur la confidentialité et les données.	• La solution CIAM prend-elle en charge les normes ouvertes basiques et avancées, notamment OAuth2, OpenID Connect, SAML, UMA 2.0, OAuth2 Device Flow et OAuth 2.0 Proof-of-Possession, FIDO2, WebAuthN et CIBA ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Accès contextuel	La plupart des solutions d'identité ne protègent que lors de l'authentification initiale. Pour garantir l'authenticité des utilisateurs, des appareils, des objets et des services à tout moment et atténuer les risques dès qu'une anomalie est détectée, même pendant les sessions existantes, il faut appliquer l'accès contextuel. L'accès contextuel intègre l'intelligence contextuelle dans les politiques afin d'évaluer les risques et de protéger les ressources au moment de l'accès ainsi qu'à tout moment au cours d'une session numérique. Il permet d'appliquer des politiques d'autorisation granulaires, le risque adaptatif, l'authentification multifactorielle et l'autorisation « push », mais n'exige ces mécanismes d'authentification plus forts que lorsque cela est nécessaire pour faciliter la tâche des utilisateurs tout en maintenant la sécurité du système. Cette capacité est utilisée pour acquérir des clients plus rapidement, offrir de meilleures expériences et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention et à la cybercriminalité.	• La solution exploite-t-elle les facteurs d'authentification et d'autorisation contextuels à n'importe quel moment de la session pour évaluer le risque - en n'invoquant des mécanismes d'authentification plus forts seulement lorsque cela est nécessaire, en évaluant qui est l'utilisateur et son contexte ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Orchestration de l'identité sans code	Les méthodes traditionnelles d'authentification et d'autorisation comprennent les noms d'utilisateur et les mots de passe, ainsi que des éléments de données validés par des tiers, tels que les numéros de sécurité sociale et les dates de naissance. Or, dans un modèle de sécurité Zero Trust, on suppose que ces authentificateurs peuvent être compromis. De plus, les méthodes traditionnelles entravent la bonne expérience de l'utilisateur. Pour proposer des parcours sécurisés et fluides aux utilisateurs, une solution CIAM doit fournir aux entreprises un outil d'orchestration d'identité sans code. Avec une interface en glisser-déposer, l'outil no-code permet aux administrateurs d'assembler et d'ajuster facilement les workflows pour les étapes telles que l'inscription, l'authentification, l'autorisation, le self-service, etc. dans les parcours des utilisateurs. Cette capacité signifie que les utilisateurs bénéficieront d'expériences hautement adaptées et personnalisées sur l'ensemble des canaux et des marques ou branches. L'orchestration de l'identité sans code donne également aux administrateurs la possibilité de créer des workflows d'authentification qui configurent, mesurent et ajustent facilement les parcours de connexion des utilisateurs à l'aide de signaux numériques, notamment les appareils, les facteurs contextuels, comportementaux, les choix de l'utilisateur, les analyses et les facteurs de risque. Les administrateurs peuvent également utiliser rapidement des authentificateurs prêts à l'emploi, utiliser des authentificateurs existants et s'intégrer à des solutions de cybersécurité. Cette capacité est utilisée pour acquérir des clients plus rapidement, offrir des expériences exceptionnelles et protéger les utilisateurs et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, aux générations Z et Alpha, ainsi qu'à la cybercriminalité.	• La solution permet-elle de créer, de visualiser et de modifier facilement les parcours d'inscription, d'autorisation et d'authentification grâce à une fonctionnalité de glisser-déposer sans code, par le biais de workflows et d'arbres (trees) ? • Comment la solution configure, mesure et ajuste les parcours d'authentification à l'aide de facteurs et de signaux numériques (contexte, risque, comportement, choix, analyse) pour non seulement déterminer le risque, mais aussi améliorer l'expérience utilisateur et informer les utilisateurs des applications en aval des connaissances accumulées au cours du parcours d'authentification ? • Comment la solution permet-elle de pré-identifier le signal numérique d'un utilisateur, comme l'emplacement, l'adresse IP, le type d'appareil, le système d'exploitation, le type de navigateur, et plus encore, avant même qu'un nom d'utilisateur ne soit collecté ? • La solution fournit-elle des authentificateurs OOB, la possibilité de créer des authentificateurs personnalisés, et dispose-t-elle d'une intégration rapide centralisée avec des fournisseurs tiers d'authentification, de gestion de la fraude et des risques? • La solution inclut-elle une autorisation transactionnelle pour les transactions à haut risque au sein d'une session ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Authentification sans mot de passe	L'utilisateur moyen possède plus de 90 comptes. Il est difficile de se souvenir de tous ces mots de passe, c'est pourquoi plus de 50 % des utilisateurs réutilisent les mêmes mots de passe sur plusieurs sites web. La création de mots de passe reposant sur des informations personnelles rend les comptes vulnérables aux attaques. L'utilisation d'un système de gestion des mots de passe est un moyen de résoudre le problème, mais certains de ces services sont eux-mêmes vulnérables. Les principales plateformes de CIAM permettent aux organisations de concevoir des parcours de connexion sécurisés et transparents sans avoir besoin de mots de passe. Certaines solutions CIAM éliminent également le besoin de noms d'utilisateur. L'authentification sans mot de passe réduit le champ d'attaque d'une entreprise en éliminant virtuellement le vol d'informations provenant d'attaques de phishing, de la réutilisation de mots de passe, des enregistreurs de frappe, etc. Cette capacité est utilisée pour offrir de meilleures expériences et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, aux générations Z et Alpha, à la cybercriminalité et à l'opinion publique.	• Comment la solution CIAM permet-elle à un administrateur d'ajouter un service d'authentification sans mot de passe au parcours d'un utilisateur ? Quelles sont les étapes que l'administrateur doit suivre ? • La solution d'authentification sans mot de passe du fournisseur de CIAM peut-elle être utilisée à la fois pour la connexion initiale et l'authentification progressive, y compris pour l'autorisation transactionnelle ? • La solution CIAM inclut-elle l'authentification sans nom d'utilisateur ?
Atténuation des fraudes	Bien qu'aucune solution unique ne puisse traiter tous les aspects de la fraude en ligne, une combinaison d'infrastructure de sécurité et de fonctions de CIAM peut détecter le vol d'informations d'identification, l'utilisation abusive de comptes privilégiés et la fraude aux transactions. Pour prédire si une fraude est probable, il faut un contexte. Les plateformes CIAM doivent permettre aux entreprises de concevoir des parcours utilisateur qui détectent les anomalies avant et après l'authentification de l'utilisateur. Les signaux de fraude et de menace comprennent la localisation de l'utilisateur, son adresse IP, le type d'appareil, le fait que l'appareil soit jailbreaké ou enraciné, le système d'exploitation, le type de navigateur, les attributs du profil de l'utilisateur, le cookie de l'appareil, la dernière connexion, l'en-tête de la demande, l'heure de la journée et l'empreinte de l'appareil. Les signaux supplémentaires après authentification comprennent le nombre de tentatives d'authentification, l'heure de la journée et la distance entre l'ordinateur de l'utilisateur et son facteur MFA. Les solutions CIAM peuvent également s'intégrer à des technologies tierces afin de réduire davantage le risque et le coût de la fraude. Cette capacité est utilisée pour protéger les clients et l'entreprise. Elle répond aux tendances liées à la cybercriminalité et à l'opinion publique.	• Comment la solution CIAM rassemble-t-elle les signaux de fraudes et de menaces pour insuffler un contexte à une session avant que l'utilisateur ne s'authentifie ? • Comment la solution capture-t-elle et stocke-t-elle des signaux supplémentaires après l'authentification pour informer les applications en aval ? • La solution CIAM peut-elle ajouter un nœud Google reCAPTCHA dans un parcours d'enregistrement pour exiger l'intervention de l'utilisateur et réduire les attaques automatisées/de robots ? • Comment la solution CIAM permet-elle une authentification renforcée et une autorisation transactionnelle pour les transactions se produisant en dehors du contexte normal de l'appareil, du lieu ou du comportement d'un utilisateur ? • La solution CIAM évalue-t-elle les sessions utilisateur présentant un niveau de suspicion élevé, moyen ou faible, et envoie-t-elle les utilisateurs présentant un risque élevé vers une version « honeypot » de la cible visée ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Analytique des connexions et logique de décision	La seule façon d'améliorer et de sécuriser en continu le parcours client est de disposer d'informations reposant sur les données. Dans le cadre de l'orchestration des identités, les analyses de connexion des utilisateurs offrent des indicateurs qui analysent les interactions des utilisateurs finaux et leurs appareils sur tous les canaux et chaque business line. Les plateformes CIAM doivent donc être en mesure de surveiller les performances des services tiers d'analyse et de lutte contre la fraude qui ont un impact sur les parcours de connexion. Les plateformes doivent également permettre aux administrateurs d'optimiser le parcours client grâce à des analyses contextuelles et comportementales qui étudient les appareils et les navigateurs utilisés, l'endroit d'où les utilisateurs se connectent, la durée des parcours de connexion selon le type d'utilisateurs, etc. À partir de là, les entreprises peuvent découvrir des corrélations entre les méthodes de connexion existantes pour améliorer les taux d'adoption par les clients. Cette capacité est utilisée pour acquérir des clients plus rapidement, offrir de meilleures expériences et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales et aux générations Z et Alpha.	• La solution évalue-t-elle si les connexions entraînent une augmentation des paniers abandonnés ? • La solution évalue-t-elle le temps moyen d'appel des systèmes de lutte contre la fraude ? • La solution contrôle-t-elle les performances des SLA qui ont un impact sur les parcours de connexion ? • La solution détermine-t-elle si des parcours de connexion plus courts entraînent une diminution des appels au service d'assistance ?
Profilage progressif	Plutôt que de demander à vos utilisateurs de remplir de longs formulaires d'inscription, vous pouvez mettre en œuvre le profilage progressif, une technique permettant de recueillir des informations sur les utilisateurs au fur et à mesure de leurs interactions avec votre système, sur votre site Web ou votre application. Par exemple, vous pouvez recueillir uniquement le nom, l'adresse électronique et le mot de passe de l'utilisateur lors de son inscription initiale. Plus tard, vous pourrez lui demander le nom de son entreprise et son titre. Cette capacité est utilisée pour acquérir des clients plus rapidement et offrir de meilleures expériences. Elle répond aux tendances liées aux expériences phygitales et aux générations Z et Alpha.	• La solution prend-elle en charge le profilage progressif tout au long du parcours et du cycle de vie du client ? • Comment l'administrateur de la solution CIAM configure-t-il le profilage progressif ? • Comment l'administrateur de la solution configure-t-il les rapports pour prendre en charge les tests alternatifs (A/B) (par exemple, comment le taux d'abandon lors de l'inscription s'améliore-t-il avec une modification des pages d'inscription) ? • Comment l'administrateur de la solution configure-t-il le support des comptes de premier niveau (utilisateurs non authentifiés et non enregistrés) ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Intégration des systèmes d'entreprise	Les plateformes CIAM sont un élément important d'un écosystème de solutions qui stocke les identités des clients et effectue la collecte et l'analyse des données. Cet écosystème comprend la gestion des identités et des accès (IAM), les systèmes de gestion des appareils mobiles (MDM), les systèmes de gestion de la relation client (CRM) et les systèmes d'automatisation du marketing. Malheureusement, la plupart de ces écosystèmes donnent lieu à des vues fragmentées du client. Les plateformes CIAM doivent pouvoir s'intégrer et se connecter à ces systèmes pour créer une vue unique du client à l'échelle de l'entreprise. Ces données agrégées fournissent un ensemble beaucoup plus robuste avec lequel il est possible d'engager les clients, par exemple en utilisant les données de localisation du système de sécurité pour des actions marketing plus personnalisées. Cette capacité est utilisée pour acquérir des clients plus rapidement et offrir de meilleures expériences. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales et aux générations Z et Alpha.	• Pour une plus grande personnalisation et une expérience omnicanale, comment la solution s'intègre-t-elle à d'autres systèmes et permet-elle la consolidation de multiples silos d'identités pour créer une vue unique du client à l'échelle de l'entreprise ? • Comment l'administrateur configure-t-il la solution pour l'intégrer à une solution CRM (par exemple, Salesforce) ?
Privacy by Design et mécanismes de consentement	Les réglementations relatives à la protection de la vie privée telles que le RGPD imposent aux utilisateurs de contrôler leurs données personnelles, notamment en matière de confidentialité, de sécurité et de préférences d'utilisation. Pour une conformité, nationale et mondiale, il est impératif que les plateformes CIAM incluent des mécanismes de Privacy by Design et de consentement basés sur la norme UMA 2.0, ainsi que l'intégration avec d'autres logiciels qui aident à répondre aux exigences réglementaires. De tels mécanismes permettent aux utilisateurs un contrôle fin pour partager et auditer leurs données, leurs appareils et leurs objets connectés. Il est important de noter que l'interface utilisateur du mécanisme de confidentialité et de contrôle doit être intuitive et conviviale. Cette capacité est utilisée pour offrir de meilleures expériences et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'opinion publique, à la confidentialité et à la réglementation des données.	• La solution prend-elle en charge un cadre de protection de la vie privée et de consentement basé sur la norme UMA 2.0 ? • Comment la solution fournit-elle aux utilisateurs un contrôle fin pour partager et auditer leurs propres données, celles sur leurs appareils et sur leurs objets connectés ? • Comment la solution prend-elle en charge le « droit à l'oubli » qui respecte le RGPD ? • Comment l'administrateur de la solution peut-il configurer plusieurs versions des documents de consentement et forcer les clients à accepter ces versions ?

FONCTIONNALITÉS INTERMÉDIAIRES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Résidence des données	La résidence et la souveraineté des données sont des concepts liés qui couvrent les aspects juridiques du lieu de résidence des données de l'utilisateur et l'autorité légale sur les données, quel que soit leur lieu de résidence. En général, la résidence des données exige que les données personnelles d'un citoyen soient collectées, stockées et traitées uniquement à l'intérieur des frontières de son pays. Pour répondre au concept de résidence des données du RGPD, les fournisseurs de CIAM doivent permettre le stockage des données des utilisateurs dans le respect de la vie privée et la réplication fractionnée des données personnelles. Cela permet de traiter les données des utilisateurs en fonction du contexte d'une juridiction particulière. Cette capacité est utilisée pour protéger les clients et l'entreprise. Elle répond aux tendances liées à l'opinion publique et à la réglementation sur la vie privée et les données.	• La solution prend-elle en charge la résidence des données ? • Comment l'administrateur de la solution de CIAM configure-t-il la résidence des données pour les différentes zones géographiques (par exemple, stockage des données dans le bon pays, respect de la confidentialité des données au niveau mondial) ?
Modèle API First	Le modèle API First est une méthode de création de solution. Dans ce modèle, un fournisseur crée d'abord l'API, puis construit la plateforme autour d'elle. Il en résulte une moindre complexité pour les développeurs et les entreprises externes. Pour des raisons de facilité d'utilisation, d'évolutivité et de flexibilité, les fournisseurs de gestion des identités numériques doivent appliquer ce modèle de développement API first pour créer un cadre API REST commun à l'ensemble de la plateforme, afin de fournir une méthode unique et commune pour invoquer tout service d'identité. Le résultat devrait être un moyen simple et sécurisé d'étendre l'identité à tous les domaines, y compris le social, le mobile, le cloud et l'IoT. Ce modèle permet d'acquérir des clients plus rapidement et de proposer de meilleures expériences. Il répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales et à l'IoT.	• Le fournisseur utilise-t-il un modèle de développement API first pour créer un cadre API REST commun à l'ensemble de la plateforme ? • Comment la solution CIAM fournit-elle une méthode unique et commune pour invoquer les services d'identité ?
Un solide écosystème de partenaires	Pour répondre aux huit tendances présentées en introduction (et à d'autres), les solutions CIAM les plus performantes sont celles qui fonctionnent parfaitement avec une grande variété d'autres technologies afin de répondre aux objectifs uniques de chaque entreprise. À ce titre, les fournisseurs de solutions CIAM doivent disposer d'un solide écosystème de partenaires respectés en matière de conseil, de technologie et d'intégration. Cet écosystème doit inclure des intégrations préconstruites, testées, toujours à jour et prêtes à être utilisées facilement. Cet attribut est utilisé pour acquérir des clients plus rapidement, offrir de meilleures expériences et protéger les clients et l'entreprise. Il répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, à l'IoT, aux générations Z et Alpha, à la cybersécurité et à la réglementation sur la confidentialité et les données.	• Le fournisseur dispose-t-il d'un solide écosystème de partenaires respectés en matière de conseil, de technologie et d'intégration ? • Combien d'intégrations sont préconstruites, testées et mises à jour ? • Les intégrations partenaires sont-elles incluses dans la plateforme CIAM sans frais supplémentaires ?

Fonctionnalités avancées

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Flexibilité de l'interface utilisateur	L'interface utilisateur (UI) pour les boîtes de connexion, les pages de profil, les interfaces de réinitialisation de mot de passe, etc., est un élément important d'une stratégie CIAM qui favorise la facilité d'utilisation dans le cadre d'une expérience digitale de qualité. L'interface utilisateur de la solution doit être intégrée dans la stratégie globale d'interface utilisateur de l'entreprise. Il est naturel que ces stratégies évoluent. Cet attribut est utilisé pour acquérir des clients plus rapidement et offrir des expériences exceptionnelles. Il répond aux tendances liées à l'économie de la réinvention, aux expériences phygitales et aux générations Z et Alpha.	• La solution CIAM permet-elle aux entreprises de créer une interface utilisateur sur mesure, c'est-à-dire la possibilité d'appeler des API REST ? • Comment la solution CIAM utilise-t-elle les SDK pour intégrer plus facilement l'identité ? • La plateforme CIAM comprend-elle des options flexibles d'interface utilisateur hébergée ?
Multimarque / Multicanal / Cross-canal **(Thématisation de l'UI)**	Chaque utilisateur est unique et doit être traité en conséquence. Un groupe possédant plusieurs marques et/ou canaux de ventes doit pouvoir reconnaître chaque utilisateur et lui offrir une expérience personnalisée. De plus, les entreprises faisant partie d'écosystèmes multipartites doivent gérer séparément et discrètement différentes unités commerciales ou groupes d'utilisateurs dans leur hiérarchie d'identité. Elles peuvent aussi avoir besoin d'étendre certains privilèges aux partenaires pour mieux gérer leurs propres clients finaux (B2B2C). Une solution de CIAM doit inclure une thématisation multimarque de l'interface utilisateur qui permet aux entreprises de définir des parcours uniques qui relient les utilisateurs au canal ou à la marque appropriée. Elle doit également prendre en charge les niveaux hiérarchiques d'utilisateurs et les administrateurs délégués. Cette capacité est utilisée pour acquérir des clients plus rapidement et offrir des expériences exceptionnelles. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales et aux générations Z et Alpha.	• Comment la solution personnalise-t-elle les thèmes de l'UI pour l'utilisateur final ? • La solution CIAM peut-elle sélectionner dynamiquement un thème en fonction de la langue ? • La solution CIAM peut-elle détecter l'organisation dont l'utilisateur est membre, et présenter une interface thématique qui correspond à cette organisation ? • La solution CIAM peut-elle détecter que l'utilisateur a une déficience visuelle et passer à un thème à fort contraste ?

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Conception d'organisations hiérarchiques, multimarques et complexes	La plupart des entreprises créent une hiérarchie de services ou de business lines pour structurer leur activité. Ces hiérarchies déterminent la manière dont elles délèguent ensuite l'administration et les droits d'accès aux utilisateurs au sein de ces organisations. La fonction de conception d'organisations hiérarchiques, multimarques et complexes offre aux entreprises la souplesse nécessaire pour mettre en place des configurations uniques de gestion des identités et des accès, comme des politiques de mots de passe et des autorisations d'accès, pour différents publics. Pour ce faire, elle permet la création de niveaux hiérarchiques d'utilisateurs et d'administrateurs délégués pour mettre en place et gérer des groupes d'utilisateurs distincts pour répondre à leurs besoins commerciaux. Les hiérarchies peuvent elles-mêmes être imbriquées dans d'autres hiérarchies selon les besoins. Des propriétaires et des administrateurs sont affectés à chaque hiérarchie, qui ont la possibilité de gérer finement les privilèges d'accès et d'autorisation des utilisateurs à leur niveau. Un administrateur d'une organisation peut avoir un accès complet aux utilisateurs de cette organisation, mais aucun accès aux utilisateurs d'une organisation adjacente. Cela permet à chaque administrateur de la hiérarchie d'apporter les changements nécessaires pour répondre aux besoins de sécurité, de convivialité et de commodité de ses utilisateurs. Cette approche permet aux entreprises d'économiser du temps et de l'argent en leur permettant de consolider plusieurs types d'identités dans un seul système. Cette capacité est utilisée pour acquérir des clients plus rapidement, offrir des expériences exceptionnelles et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires et à la cybersécurité.	• La solution CIAM prend-elle en charge des configurations uniques de gestion des identités et des accès pour différentes hiérarchies ou business lines ? et comment ? • Comment l'administrateur configure-t-il la solution pour prendre en charge plusieurs marques ou propriétés en ligne de la même entreprise mère ? Faites la démonstration de la liaison des comptes. • Comment l'administrateur de la solution crée-t-il une nouvelle organisation pour le multi-tenant (il s'agit généralement d'une exigence lorsqu'un MSSP ou une très grande entreprise utilise la solution CIAM et doit s'assurer que certains administrateurs ne disposent que de privilèges d'administration pour certains clients ou organisations internes) ?

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Sécurité Zero Trust	Le modèle de sécurité Zero Trust repose sur l'idée qu'aucun réseau, individu, appareil ou objet n'est digne de confiance. Les plateformes CIAM devraient pouvoir déterminer si une entité qui souhaite effectuer une action est vraiment autorisée à le faire et si elle a prouvé qu'elle est vraiment l'entité qu'elle prétend être, avec un niveau d'assurance suffisant, compte tenu du risque lié à l'action en question. Dans un modèle de sécurité Zero Trust, chaque action entreprise doit être correctement authentifiée et autorisée. Pour ce faire, les décisions d'authentification et d'autorisation s'appuient sur des informations contextuelles. Elles ne sont plus binaires mais reposent sur le niveau de risque, en tenant compte d'un riche ensemble d'informations. Cette capacité est utilisée pour offrir des expériences exceptionnelles et pour protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires et à la cybercriminalité.	• La solution fournit-elle les modèles de sécurité Zero Trust et CARTA (authentification adaptative) ? • Comment permet-elle aux personnes, aux appareils, aux objets et aux applications de disposer de différents niveaux d'informations d'identification pour s'authentifier auprès d'un identity store commun ? • Comment l'administrateur de la solution CIAM configure-t-il l'évaluation des risques en utilisant les attributs des appareils à haut risque (y compris, mais sans s'y limiter, le jailbreaking, les logiciels malveillants, les émulateurs, le JavaScript désactivé, les cookies volés d'une autre session) ? • Comment l'administrateur de la solution CIAM configure-t-il les scores de risque utilisés pour piloter les politiques d'authentification (par exemple, le client se connecte à partir d'un pays inhabituel, ou se connecte à partir d'un tout nouvel appareil, les connexions du client montrent des voyages peu plausibles, etc.) Quels types de sources de menaces propres et tierces (mauvaises adresses IP, etc.) sont disponibles dans la solution ? • Comment l'administrateur de la solution configure-t-il la protection des clients contre les attaques de type credential stuffing et password spraying ?
Conception distribuée de la portée avec accès le moins privilégié	Les portées (scopes) permettent d'appliquer le principe de « l'accès le moins privilégié ». Cela signifie que l'on n'accorde que l'accès indispensable à la réalisation d'un objectif donné. Par exemple, les clients ne sont autorisés à accéder qu'aux informations et ressources exactes nécessaires à un objectif particulier et légitime. Une première étape vers la réalisation de cette autorisation granulaire consiste à mettre au point un mécanisme permettant de « distribuer » et d'attribuer des portées fortement typées aux applications, aux endpoints des API et aux autres ressources protégées. Les portées doivent ensuite être associées à un contexte en temps réel aux points d'application des politiques dans l'ensemble de l'écosystème de l'identité. Il convient également d'appliquer des portées pour des règles précises et exploitables qui peuvent être utilisées pour prendre des décisions d'autorisation. Cette capacité est utilisée pour protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes partenaires et à la cybercriminalité.	• Comment la solution permet-elle d'appliquer le principe de « l'accès le moins privilégié » pour n'accorder que l'accès essentiel à l'accomplissement d'un objectif donné ? • Comment la solution peut-elle accorder des portées à différents groupes d'utilisateurs en se basant sur leur structure organisationnelle (emplacement, hiérarchie, business line) ?

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Agrégation de données sur les personnes, les objets et leurs relations	Pour créer des expériences omnicanales sécurisées et personnalisées, les fournisseurs de CIAM doivent permettre aux entreprises d'agréger les données relationnelles entre les personnes et leurs objets IoT pour créer une vue unique et très complète de leurs clients. Pour ce faire, il faut répondre à plusieurs exigences techniques, notamment établir un modèle de données client commun, connecter un large éventail de sources de données, mettre en œuvre une logique de synchronisation et de réconciliation simple et permettre l'accès aux données client dans un format approprié. Cette capacité est utilisée pour offrir des expériences exceptionnelles et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, aux expériences phygitales, à l'IoT, aux générations Z et Alpha, ainsi qu'à la cybercriminalité.	• La solution inclut-elle la modélisation des relations d'identité à un niveau granulaire (parents, enfants, amis, IoT, etc.) pour la gestion des identités entre ces relations ?
Sécurité périphérique	Comme nous l'avons vu précédemment, la plupart des objets IoT ne sont pas sécurisés. La solution gère la périphérie et sécurise les appareils et les données qu'ils collectent grâce aux contrôleurs de périphérie et aux agents de messages (IMB). Les contrôleurs de périphérie sécurisent les identités IoT et les informations d'identification qui leur sont associées afin qu'elles soient fiables et utilisables dans de nombreux écosystèmes connectés pour prévenir les attaques de type « man-in-the-middle » et autres. De nombreux objets IoT utilisent des protocoles non sécurisés tels que MQTT pour s'identifier et envoyer et recevoir des informations. Les Identity Message Brokers sécurisent ces protocoles en convertissant MQTT, et d'autres protocoles, en HTTPS et en permettant l'authentification et l'autorisation des appareils et des données. Cette capacité est utilisée pour offrir des expériences exceptionnelles et protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux expériences phygitales, à l'IoT et à la cybercriminalité.	• La solution utilise-t-elle des contrôleurs de périphérie pour sécuriser les identités IoT et leurs informations d'identification associées afin qu'elles soient fiables et utilisables dans de nombreux écosystèmes connectés pour prévenir les attaques de type « man-in-the- middle » et autres types d'attaques ? • La solution utilise-t-elle des agents de messages pour sécuriser les protocoles IoT, tels que MQTT vers HTTPS afin de rendre possible l'authentification et l'autorisation de l'objet IoT et des données ?

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Support des applications existantes	La plupart des entreprises détiennent un grand nombre de systèmes et d'applications hérités. Nombre d'entre eux stockent les données et les informations d'identification des clients, mais ne disposent que de capacités limitées voire inexistantes pour l'inscription, l'authentification, l'autorisation ou la fédération des utilisateurs. Par conséquent, la possibilité de se connecter et de s'étendre aux systèmes et applications existants avec un système d'identité moderne est une caractéristique importante des plateformes CIAM. Cela se fait par le biais d'une passerelle d'identité, qui permet aux systèmes et applications anciens et récents de communiquer entre eux de manière fluide et sécurisée. Cette capacité est utilisée pour offrir des expériences exceptionnelles. Elle répond à la tendance de l'économie de la réinvention.	• La solution a-t-elle la capacité de se connecter et de s'étendre aux systèmes et applications existants via une passerelle d'identité ? • Comment la passerelle d'identité du fournisseur CIAM s'intègre-t-elle aux applications existantes qui ne sont pas conçues pour fonctionner avec des solutions de gestion des accès ou d'authentification unique (SSO) ? • Comment la passerelle d'identité du fournisseur CIAM permet-elle une intégration sécurisée entre les applications anciennes et récentes ?
Architecture DevOps-friendly et microservices	Le DevOps permet le développement et le déploiement de logiciels en cycle continu, ce qui permet aux entreprises de déployer de nouvelles fonctionnalités plus rapidement en réduisant le temps de mise en production. Les fournisseurs de CIAM doivent proposer une architecture adaptée au DevOps, avec la possibilité d'exploiter les outils DevOps, tels que l'automatisation et l'orchestration du déploiement d'un simple clic et en continu. Ils doivent également utiliser des images conteneurisées pour une automatisation rapide, avec la prise en charge de Docker, et disposer d'une architecture intelligente qui sépare la configuration des binaires afin d'exploiter facilement le contrôle de version pour les artefacts DevOps. En outre, les fournisseurs doivent fournir des outils de ligne de commande pour la configuration à distance. Les microservices sont une autre méthode de développement importante qui se concentre sur la construction et le déploiement d'applications sous forme de groupes de services modulaires et composables au sein d'une application. L'avantage des microservices est la possibilité de modifier singulièrement un service sans que cela ait un impact sur les autres. Ces capacités sont utilisées pour acquérir des clients plus rapidement et offrir des expériences exceptionnelles. Elles répondent à la tendance de l'économie de la réinvention.	• Comment la solution prend-elle en charge les approches DevOps et les technologies de conteneurisation et d'orchestration telles que Docker et Kubernetes ? • Comment la solution CIAM sécurise-t-elle les microservices ? • Comment la solution CIAM évolue-t-elle horizontalement et verticalement ?

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Modèles d'architecture sans serveur	Comme nous l'avons vu dans la section sur la disponibilité et l'évolutivité, les entreprises doivent tenir compte de divers scénarios d'évolutivité, tels que des millions de sessions simultanées. Pour y parvenir de manière rentable, les principaux fournisseurs de solutions de gestion des identités numériques adoptent les modèles d'architecture sans serveur. L'architecture sans serveur permet non seulement aux serveurs d'augmenter ou de réduire leur capacité en fonction des besoins, mais aussi de baser les conditions de location des centres de données sur la taille de la mémoire utilisée sur un serveur ainsi que sur la durée d'utilisation de celle-ci. Grâce à cette méthode, les développeurs n'ont plus besoin de gérer de grandes quantités de serveurs qui ne sont utilisés que périodiquement, lors des pics de charge. Cette capacité est utilisée pour réduire les coûts et répondre à la tendance liée à l'économie de réinvention.	• La solution prend-elle en charge les modèles d'architecture sans serveur ? • La solution prend-elle en charge le modèle d'application web (REST, GraphQL), les modèles ETL (extraction, transformation, chargement) tels que FanOut, les modèles de big data (tels que MapReduce) et les modèles d'automatisation et de déploiement (tels que CI/CD) ?
Multi-cloud et cloud hybride	Les environnements multi-cloud sont devenus populaires en raison de leur flexibilité, de leur disponibilité et de leur évolutivité accrues. Ces environnements permettent aux entreprises d'éliminer le verrouillage des fournisseurs et d'accélérer la mise sur le marché tout en réduisant la complexité et en économisant du temps et de l'argent. Les environnements hybrides comprennent à la fois des environnements sur site et des environnements dans le cloud. Les environnements dans le cloud répondent aux besoins évolutifs, tandis que les environnements sur site sont conseillés pour stocker les données sensibles pour une meilleure sécurité. L'avantage des environnements hybrides est la flexibilité qui permet de prendre en charge n'importe quel déploiement, n'importe où et à tout moment. Les plateformes CIAM doivent inclure ces options flexibles de déploiements multi-cloud et hybride. Ces options répondent à la tendance de l'économie de réinvention.	• Comment la solution peut-elle être déployée dans n'importe quel environnement cloud, y compris multi-cloud, bring- your-own-cloud, ou cloud hybride ? • Comprend-elle une configuration hautement disponible et prête pour la production ? • Comment fonctionnent les licences pour prendre en charge un modèle de cloud hybride ?

FONCTIONNALITÉS AVANCÉES	DÉFINITIONS ET IMPORTANCE	LES QUESTIONS À POSER AUX FOURNISSEURS
Audit et analyse du système	Les capacités d'audit et d'analyse des systèmes sont des fonctions essentielles. Les plateformes CIAM doivent être en mesure de réaliser des audits pour la sécurité des systèmes, le dépannage, l'analyse de l'utilisation et la conformité réglementaire. Elles doivent également prendre en charge un large éventail de fonctions de surveillance et de connexion. Les journaux d'audit doivent rassembler des informations opérationnelles sur les événements survenant dans un déploiement afin de suivre les processus et les données de sécurité, y compris les mécanismes d'authentification, l'accès au système, l'activité des utilisateurs et des administrateurs, les messages d'erreur et les changements de configuration. De plus, les plateformes CIAM doivent fournir des audits et des analyses pour les systèmes avec lesquels elles travaillent, comme les systèmes partenaires. Cette capacité est utilisée pour protéger les clients et l'entreprise. Elle répond aux tendances liées à l'économie de la réinvention, aux écosystèmes de partenaires, à l'IoT, à la cybercriminalité et à la réglementation sur la vie privée et les données.	• La solution permet-elle d'effectuer des audits de la sécurité du système, du dépannage, ou de de l'utilisation et de la conformité réglementaire ? • La solution peut-elle également prendre en charge un large éventail de fonctions de surveillance et de connexions ?

ForgeRock : Le leader incontesté du CIAM d'entreprise

En tant que leader incontesté du CIAM, ForgeRock aide les entreprises les plus ambitieuses à répondre aux tendances liées à la transformation digitale pour acquérir des clients plus rapidement, offrir des expériences exceptionnelles et protéger les clients et l'entreprise. Avec ForgeRock, vous pouvez améliorer votre activité grâce à la seule plateforme complète du marché, utilisant l'intelligence artificielle et conçue pour toutes les identités et tous les clouds.

« En avril 2020, nous avons lancé BBC Bitesize, un site Web qui fournit aux parents et aux élèves des vidéos gratuites, des guides, des activités et des quiz, par niveau et par sujet. Nous avons relancé le service en quelques semaines et vu trois millions de personnes l'utiliser le jour du lancement, sans aucun temps d'arrêt. »

Matt Gres, Directeur de la plateforme BBC

FORRESTER®

LEADER

Forrester Wave™ Customer Identity and Access Management, quatrième trimestre 2022

Gartner®

HIGHEST SCORE

Gartner® Critical Capabilities for External Access Management, 2022

kuppingercole ANALYSTS

OVERALL LEADER

KuppingerCole Leadership Compass, Customer Identity and Access Management, 2022

Les entreprises mondiales stimulent leur croissance avec ForgeRock Enterprise CIAM. Rejoignez la communauté ForgeRock et soutenez vos initiatives uniques de réinvention pour répondre non seulement aux tendances d'aujourd'hui, mais aussi à celles de demain.

« Chez Philips, nous avons pour mission d'améliorer la vie des gens et de leur donner les moyens de mieux prendre soin d'eux-mêmes et des autres. Avec ForgeRock, nous sommes en mesure de concevoir des technologies innovantes de partage des données et de consentement sur notre plateforme numérique HealthSuiteDigital qui favorisent la confiance des consommateurs et des patients. »

Jeroen Tas,
Directeur de l'innovation et de la stratégie

PHILIPS

Et maintenant ?

En savoir plus sur ForgeRock et le CIAM

- **Découvrez** comment HSBC offre des expériences utilisateur sécurisées et personnalisées à plus de 30 millions de clients dans 36 pays.
- **Regardez** le webinaire de ForgeRock et Deloitte : *Quatre technologies pour concevoir des parcours numériques CIAM captivants*
- **Contactez-nous** pour entamer un échange et organiser une démonstration

« C'est le moment de migrer vers le cloud, de profiter de l'IA et de l'infrastructure de nouvelle génération ; l'architecture que les entreprises mettent en place aujourd'hui déterminera leur avenir. »[9]

accenture

Ressources indépendantes

Consultez ces rapports d'analystes pour découvrir pourquoi ForgeRock est le leader du CIAM :

- **Forrester Total Economic Impact™ Study** of ForgeRock Customer Identity and Access Management
- **The Forrester Wave™** : Gestion des identités et des accès des clients, 2022
- **Gartner®** : Fonctionnalités stratégiques pour la gestion des accès, 2022
- **KuppingerCole Leadership Compass** : Plateformes CIAM, 2022

- Pour des formations et des conseils sur le marché et les technologies du CIAM, visitez **The Cyber Hut**.

9 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf

About ForgeRock

ForgeRock®, (NYSE: FORG) est un leader mondial de l'identité numérique qui propose des solutions complètes et innovantes pour la gestion des identités et des accès permettant aux clients, aux collaborateurs et aux appareils d'accéder simplement et en toute sécurité au monde connecté. Grâce à ForgeRock, plus de 1 300 entreprises dans le monde orchestrent, gèrent et sécurisent le cycle de vie complet des identités - depuis les contrôles d'accès dynamiques jusqu'à la gouvernance, en passant par les API et le stockage de données d'authentification - utilisables dans tout environnement, cloud ou hybride. La société est présente dans le monde entier, avec son siège mondial à San Francisco, en Californie. Pour plus d'informations et téléchargements gratuits, visitez **www.forgerock.com**.

Suivez-nous :

ForgeRock