ForgeRock®

Les 8 tendances qui façonnent la transformation digitale des entreprises et de la société

Pourquoi les tendances en matière de consommation font de la gestion des identités et des accès clients (CIAM) un impératif ?

Introduction

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 et au-delà, les organisations doivent être équipées pour faire face à chacune d'elles.

1. Disruption. L'économie de la réinvention

La pandémie a tout bouleversé. Aujourd'hui, 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 clients interagissent avec une entreprise, ils veulent une expérience fluide et transparente qui allie les éléments physiques et numériques.

4. Internet des Objets (IoT)

Le marché mondial de l'IoT grand public devrait passer de 97,50 milliards de dollars en 2020 à une estimation de 188,34 milliards de dollars d'ici à 2026[1]. Malheureusement la plupart de ces « objets » ne sont pas sûrs.

5. Cybercriminalité, failles, fraudes…

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 apprendront, y feront des achats et y investiront !

Pour suivre ces tendances, les plus grandes entreprises se tournent vers les plateformes de gestion des identités conçues spécialement pour les consommateurs, l'IoT, leurs collaborateurs et les autres cas d'utilisation qui apparaîtront dans l'avenir.

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/

ForgeRock : le leader incontesté du CIAM

Reconnu consécutivement par Gartner, Forrester et KuppingerCole pour la gestion des identités externes et la gestion des identités et des accès clients (CIAM), ForgeRock propose la seule solution du marché capable d'accompagner ses clients pour répondre aux nouvelles tendances et être préparés pour l'avenir.

La solution de ForgeRock permet aux entreprises de :

- réinventer leurs stratégies commerciales et informatiques pour faire face à tout type de perturbation et répondre aux demandes des consommateurs avec agilité et résilience en fonction du besoin,
- faire partie, en toute sécurité, d'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 enseignes 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 demande des générations qui arrivent sur le marché.

Grâce à ForgeRock, les entreprises peuvent non seulement affronter ces tendances, mais aussi les devancer. La solution CIAM de ForgeRock offre de nouvelles opportunités d'accroître le chiffre d'affaires grâce à des fonctionnalités conçues pour permettre des expériences clients qui dépassent leurs attentes, pour réduire les risques et les fraudes grâce à l'approche Zero Trust, et pour développer la confiance et une fidélité digitale accrue grâce à une attention particulière portée à la conformité règlementaire en matière de confidentialité et de consentement.

Table des matières

Les 8 tendances qui façonnent la transformation digitale des entreprises et de la société

Pourquoi les tendances en matière de consommation font de la gestion des identités et des accès clients (CIAM) un impératif ?

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 et au-delà, les organisations doivent être équipées pour faire face à chacune d'elles.

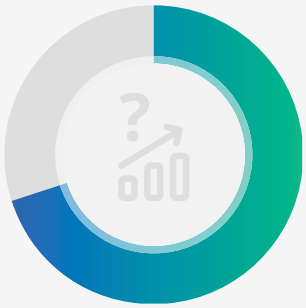
1

Disruption. L'économie de la réinvention

Pour comprendre « l'économie de la réinvention », il faut comprendre « l'économie de la disruption ». Les consommateurs veulent des expériences multicanales irréprochables et personnalisées. Pour répondre à cette demande et devancer la concurrence, les entreprises déploient d'énormes efforts pour innover avec de nouveaux services et en peaufinant les expériences.

Par exemple, en 2005, Amazon a été disruptif avec Prime, promettant la livraison gratuite en deux jours pour ses membres.

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.[3]



Deloitte.

Plus de 15 ans plus tard, d'autres retailers aspirent toujours à rivaliser pour combler cette attente désormais courante des consommateurs.

La nature inhérente de l'économie disruptive est d'être en constante évolution. Les entreprises développent de nouveaux moyens innovants de servir et satisfaire leurs clients. En retour, les consommateurs s'adaptent aux nouvelles innovations et les transforment en attentes - ce qui incite les entreprises à innover encore en pensant à la prochaine nouveauté.

La relation intime qui lie innovation digitale et attentes des consommateurs oriente et façonne la société depuis plus de deux décennies. Avant la pandémie de Covid-19, la capacité à offrir des expériences client multicanales, personnalisées et sans failles était le moteur de la transformation digitale dans tous les secteurs d'activité. Pour la plupart des entreprises, la planification et l'exécution de ces initiatives se sont étalées sur des années. Cependant, lorsque la pandémie a frappé, les services en ligne sont devenus une façon de vivre à la fois pour les citoyens et les entreprises. En un instant, les délais envisagés pour la transformation digitale sont passés de plusieurs années à quelques semaines. Les entreprises qui ont pris de l'avance sont celles qui disposaient d'infrastructures informatiques déjà modernisées et d'offres de services numériques capables de répondre à la demande des consommateurs dès le premier jour.

L'économie de la réinvention est née de la disruption ultime causée par la pandémie.

3 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

Dans le monde entier, la pandémie a déclenché une urgence dans la transformation digitale des entreprises. Avec une demande de biens de consommation et de services en forte hausse et une chaîne d'approvisionnement en plein chaos, les entreprises mondiales sont engagées dans une course pour acquérir et fidéliser les clients, atténuer leurs pertes et assurer l'avenir de leur activité.

83%

des cadres s'accordent à dire que les stratégies commerciales et technologiques de leur organisation sont de plus en plus indissociables, voire même qu'elles sont indiscernables.[4]

accenture

Afin d'être compétitives et de servir les clients dans un monde avant tout numérique, les entreprises consacrent des ressources sans précédent à l'amélioration de la qualité de leurs services et se réinventent pour devenir plus intelligentes, plus agiles et plus résilientes. Par exemple, elles revoient leurs infrastructures informatiques et migrent dans le cloud lorsque c'est possible ; elles intègrent des capteurs, des balises et des appareils de l'Internet des Objets (IoT) ; elles mettent en œuvre l'intelligence artificielle (IA), l'apprentissage automatique (ML) et l'automatisation du traitement robotique (RPA) ; et elles créent des jumeaux numériques et des mondes en miroir.

L'expérience du consommateur régnant en maître, les efforts massifs déployés dans le cadre de l'économie de la réinvention visent à préparer les entreprises à affronter le monde, non seulement celui post-pandémie, mais aussi le « monde d'après ». Cet objectif ambitieux demande d'allier la stratégie de l'entreprise aux solutions technologiques innovantes.

Il est essentiel de se doter des capacités nécessaires pour construire l'organisation résiliente du futur, capable de percevoir la volatilité et la disruption et capable d'y répondre.[5]

Gartner

4 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
5 Gartner, The C-Suite Guide : Accélérer le numérique pour une entreprise prête pour l'avenir. Des cadres pour les technologies composables, les clients autonomes et l'avenir du travail, 2021

2

Écosystèmes partenaires

Dans le cadre de leur réinvention, les entreprises pénètrent dans des écosystèmes numériques multipartites pour répondre à la demande insatiable des consommateurs en matière d'expériences multicanales agréables et personnalisées.

Selon McKinsey[6], les écosystèmes numériques prennent corps aujourd'hui dans sept des douze plus grandes entreprises du monde en termes de capitalisation boursière. Grâce à des technologies telles que le cloud et les interfaces de programmation d'applications (API), ces réseaux de partenaires améliorent l'efficacité opérationnelle, la transparence et l'évolutivité, étendent les offres de services et contribuent à offrir des expériences disruptives.

Prenons l'exemple d'un groupe du secteur de la santé aux États-Unis. Les prestataires de soin, les patients, les distributeurs et d'autres acteurs du secteur unissent leurs forces pour créer des services numériques qui combinent plusieurs services en une seule application pratique pour l'utilisateur final. Par exemple, une seule application permet aux patients de prendre un rendez-vous, ou de réserver une consultation de télésanté, de consulter les résultats de leurs tests, de payer leurs factures, d'avoir des rappels de soins et des conseils, et de savoir quand leurs ordonnances sont prêtes à être récupérées.

Les grandes entreprises ont appris qu'unir leurs forces pour créer des solutions permettant une expérience transparente de bout en bout tout au long du parcours client est une stratégie gagnante. Dans cet effort, les écosystèmes numériques multipartites reposent sur la sécurité des API et exigent d'accorder le niveau d'accès approprié aux systèmes et aux données au-delà des frontières de l'entreprise.

60 trillions $

Nos recherches montrent qu'un ensemble émergent d'écosystèmes numériques pourrait représenter plus de 60 000 milliards de dollars de chiffre d'affaires, d'ici à 2025, soit plus de 30 % du chiffre d'affaires mondial des entreprises.[7]

McKinsey & Company

6,7 https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-strategy-and-corporate-finance-blog/if-youre-not-building-an-ecosystem-chances-are-your-competitors-are

3

Expériences phygitales

La pandémie a eu de nombreuses conséquences, notamment une appréciation nouvelle des expériences en personne. En même temps, elle a exposé le public au confort et à la commodité des services en ligne. Aujourd'hui, on veut le meilleur des deux.

À mesure que les entreprises ré-imaginent les offres de produits et de services possibles en ligne, elles constateront qu'elles jouent un rôle plus actif que jamais dans la relation entre les personnes et la technologie.[8]

accenture

Selon Ken Hughes, éminent spécialiste du comportement des consommateurs, « il n'a jamais été aussi important d'humaniser l'expérience client. Une bonne expérience client n'est pas seulement une question de commodité, mais aussi de connexion. Le numérique peut nous apporter l'efficacité, mais la véritable connexion vient désormais de la touche humaine empathique. C'est une question de silicium et d'âme. ».[9]

Multicanal signifie désormais tous les canaux, y compris le canal physique. Quel que soit le mode d'interaction des consommateurs avec une entreprise, ils veulent une expérience personnalisée et transparente qui reprenne là où ils se sont arrêtés. Pour y parvenir, les entreprises conçoivent des expériences « phygitales », c'est-à-dire des parcours clients personnalisés composés d'éléments physiques et numériques.

Le physique + le digital, c'est le nouveau « sur mesure ». Au cours des 18 à 24 prochains mois, nous nous attendons à voir des entreprises de premier plan adopter la tendance du sur-mesure en explorant les moyens d'utiliser la conception centrée sur l'humain et la technologie numérique pour créer des interactions personnalisées et enrichies numériquement.[10]

Deloitte.

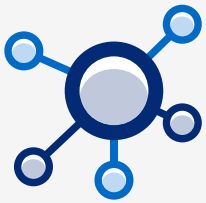
Par exemple, certains retailers envoient des messages SMS à leurs clients pendant qu'ils sont dans le magasin physique pour leur proposer des offres personnalisées ou même les diriger vers l'emplacement des produits qu'ils ont recherchés en ligne. Les restaurants proposent également des expériences phygitales en intégrant des QR codes qui affichent les menus sur les smartphones des clients. De plus, ils utilisent des applications qui permettent aux clients de fractionner facilement leurs additions. Les expériences phygitales ont également fait leur entrée dans les magasins de vêtements. Certains retailers, tels Macy's au Royaume-Uni, ont installé des miroirs intelligents à réalité augmentée (AR) dans leurs magasins physiques, qui permettent aux clients de voir comment les vêtements leur vont avant de les essayer physiquement.

Au cours des prochaines années, l'intégration des expériences « phygitales » occupera une place prépondérante dans la vie quotidienne. Pour offrir ces expériences, il est important de connaître le client à chaque point de contact et d'assurer sécurité et confiance.

8 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
9 https://kenhughes.info/wp-content/uploads/2020/11/The-captive-economy-2021.pdf
10 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

4 Internet des Objets (IoT)

Les appareils intelligents qui constituent l'Internet des Objets (IoT) sont devenus omniprésents, car les organisations de tous les secteurs innovent en proposant de nouvelles offres et expériences phygitales. D'après Market Data Forecast,[11] le marché mondial de l'IoT grand public devrait passer de 97,5 milliards de dollars en 2020 à un montant estimé à 188,3 milliards de dollars d'ici à 2026.



Les appareils de l'Internet des Objets (IoT) sont parmi les machines connectées les moins sécurisées, mais ils deviennent également omniprésents dans nos vies.[12]

WORLD ECONOMIC FORUM

Des miroirs intelligents phygitaux aux thermomètres, en passant par les matelas, les voitures, les chaussures et les jouets, les biens de consommation s'articulent de plus en plus autour des objets IoT, des données qu'ils collectent et des applications auxquelles ils se connectent.

Par exemple, Philips a développé une gamme d'ampoules intelligentes appelée Philips Hue. Ces ampoules sont connectées à l'application mobile Philips Hue, qui permet aux utilisateurs de contrôler les paramètres d'éclairage, comme la luminosité, la couleur ou l'ambiance. Les clients peuvent également connecter ces ampoules à des appareils comme Echo d'Amazon ou Nest de Google afin de régler l'éclairage en mains libres ou lorsqu'ils ne sont pas chez eux.

Si l'IoT améliore la vie des consommateurs et aide les entreprises à se différencier par des offres de services inédites, la triste réalité est que la plupart de ces objets ne sont pas sécurisés et peuvent être utilisés de manière malveillante. Les cyberattaques liées à l'IoT ont plus que doublé au premier semestre 2021 par rapport à l'année précédente, entraînant autour d'un milliard et demi de violations (au lieu des 639 millions recensées en 2020[13]).

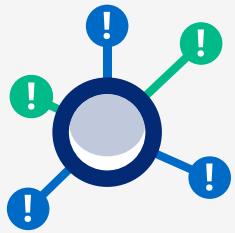
Les conséquences des piratages et des violations de l'IoT peuvent être terribles, la sécurité des identités IoT et de leurs données doit être une priorité absolue.

11 https://www.marketdataforecast.com/market-reports/consumer-iot-market
12 https://www.weforum.org/agenda/2021/08/threats-to-iot-devices-are-constantly-evolving-but-is-security-keeping-up/
13 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky

5

Cybercriminalité, failles, fraudes…

Alors que le numérique prend de l'ampleur, les tactiques de cybercriminalité et la cyberguerre évoluent elles aussi. Aujourd'hui, rien n'est plus sinistre pour une entreprise qu'un piratage, une violation de données ou une réputation entachée à cause de mauvaises pratiques de sécurité et de gestion des données. Au cours des dernières années, le nombre de failles, d'attaques par phishing, de fraudes, de ransomwares et d'atteintes à la vie privée a atteint de nouveaux sommets.



La croissance prévue des appareils intelligents, de la 5G, de l'edge computing et de l'intelligence artificielle promet de créer encore plus de données, de nœuds connectés et de champs d'attaque étendus.[14]

Deloitte.

85% Près de 85 % des violations de données réussies impliquaient une fraude humaine.[15]

80% Les applications web sont le principal vecteur d'attaque, liées à plus de 80 % des failles.[16]

61% de toutes les violations de données sont le résultat de manœuvres, telles que l'hameçonnage (phishing), qui volent les identifiants de connexion.[17]

2 Mrds 2 milliards de fichiers de données contenant des noms d'utilisateur et des mots de passe ont été compromis en 2021.[18]

136% Les cyberattaques liées à l'IoT ont augmenté de 136 % au cours du seul premier semestre de 2021.[19]

14 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf
15 https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
16 https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf
17 https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
18 https://www.forgerock.com/resources/analyst-report/2022-forgerock-consumer-identity-breach-report
19 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

Les clés couramment utilisées pour accéder à un système informatique - noms d'utilisateur, mots de passe et informations personnelles identifiables (PII) - font partie des informations les plus convoitées par les cybercriminels.

Voici quelques exemples récents notables. En 2019, des pirates ont pénétré SolarWinds avec un mot de passe volé, affectant jusqu'à 18 000 de leurs clients, dont des entreprises du Fortune 500 et des agences gouvernementales américaines. En 2020, le gouvernement américain aurait payé 400 milliards de dollars en chômage frauduleux à un réseau international de criminels.[20] En Allemagne, en 2021, le distributeur de produits chimiques Brenntag a payé une rançon de 4,4 millions de dollars pour récupérer 150 Go de dossiers médicaux et autres données sensibles volés.[21] La même année, une fuite de données de Microsoft Power Apps a touché 47 entreprises dans différents secteurs d'activité, exposant 38 millions d'enregistrements contenant des informations personnelles identifiables (PII).[22]

Si des progrès ont été constatés au cours des dernières années, les répercussions juridiques des violations de données restent souvent en deçà des attentes des consommateurs lésés. Lorsque des informations personnelles ont été volées, les consommateurs sont largement insatisfaits des compensations et des réparations qui leur sont offertes par les entreprises.

Le public est désabusé. Plus d'une décennie de failles de sécurité dans les médias a eu un impact non seulement sur la façon dont les gens perçoivent les entreprises et s'y engagent, mais aussi sur ce qu'ils y attendent en termes de sécurité, d'accès, de contrôle et d'utilisation de leurs données personnelles.

Lorsque ces responsabilités « bidirectionnelles B-to-C » ne sont pas assumées, les résultats sont pires que des clients déçus : l'échec crée une société désabusée par le modèle d'innovation intégré sur lequel les entreprises comptent pour se développer.[23]

accenture

20 https://www.forbes.com/sites/jackkelly/2021/06/12/the-most-brazen-400-billion-unemployment-funds-heist-in-history/?sh=279ec76a2020
21 https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/
22 https://healthitsecurity.com/news/microsoft-data-breach-exposes-38m-records-containing-pii
23 https://www.accenture.com/t20180227T215953Z__w__/us-en/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

6 Opinion publique et militantisme

La société est désormais méfiante. Dans ce contexte, les gens sont très conscients de la collecte de données qu'effectuent les moteurs de recherche, des cookies et des objets IoT, ainsi que de la menace que représente la cybercriminalité, avec le phishing et les fraudes. Comme le résume le Pew Research Center, ils sont « inquiets, confus et ressentent un manque de contrôle sur leurs informations personnelles[24].»

Selon notre enquête, les facteurs les plus importants pour les consommateurs lorsqu'ils partagent leurs données personnelles avec une entreprise sont les suivants : La sécurité de la collecte et du stockage des données (63 %), le contrôle de la nature des données partagées (57 %) et la confiance dans l'entreprise (51 %). Si ces garanties ne sont pas fournies par les entreprises, alors ils les chercheront ailleurs.[25]

EY

Selon plusieurs enquêtes menées par des organisations telles que le Pew Research Center, l'Agence des Droits Fondamentaux de l'Union Européenne, EY, PwC, Salesforce et RSA :

54% des consommateurs déclarent que le COVID-19 les a rendus plus conscients des données personnelles qu'ils partagent aujourd'hui qu'ils ne l'étaient avant la pandémie.[26]

54% des clients affirment qu'il est plus difficile que jamais pour les entreprises de gagner leur confiance.[27]

81% des consommateurs affirment que les risques potentiels liés à la collecte de données par les entreprises l'emportent sur les avantages.[28]

24 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
25, 26 https://assets.ey.com/content/dam/ey-sites/ey-com/es_es/topics/resilient-enterprise/ey-global-consumer-privacy-study-2020-single-pages.pdf
27 https://www.salesforce.com/form/pdf/state-of-the-connected-customer-3rd-edition/
28 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

41% des résidents de l'Union Européenne ne souhaitent pas partager leurs données personnelles avec des entreprises privées.[29]

64% des américains accusent l'entreprise, et non le pirate, lorsque leurs données sont piratées.[30]

83% des australiens souhaiteraient que le gouvernement fasse davantage pour protéger la confidentialité des données de ses citoyens.[31]

Comme l'illustrent les statistiques ci-dessus, l'opinion publique a désormais pris une posture défensive, ce qui rend l'interaction entre les entreprises et la société très importante. En conséquence, la société exige désormais plus de transparence de la part des entreprises et plaide pour l'élaboration de réglementations encore plus strictes.

Par exemple, Max Schrems, un avocat militant, a lancé des campagnes contre Facebook, maintenant appelé Meta Inc., pour violations de la vie privée et inadéquation avec le cadre du Privacy Shield de l'Union Européenne (U.E.) et des États-Unis.

L'adoption ira de pair avec la confiance pour la prochaine génération de produits et de services.[32]

accenture

La Cour de Justice de l'Union Européenne (CJEU) a statué en faveur de Schrems dans deux affaires, modifiant ainsi la manière dont les entreprises traitent les données des utilisateurs à l'échelle mondiale.

Le témoignage de la lanceuse d'alerte chez Facebook, Frances Haugen, est un autre exemple. Elle a révélé que l'entreprise avait négligé de réagir face aux recherches démontrant que les algorithmes et les tactiques utilisés sur les plateformes Instagram et Facebook sont nuisibles aux jeunes filles et aux adolescents – entre autres révélations clés. Ce témoignage a suscité un soutien aux États-Unis en faveur d'une action réglementaire. Il donne également une impulsion à la proposition de loi sur les services numériques (Digital Services Act) de l'UE, qui vise à limiter strictement les contenus illégaux, y compris la désinformation, et à contraindre l'industrie technologique à rendre plus transparents les algorithmes qui collectent les données personnelles et ciblent le contenu pour les utilisateurs.[33]

29 https://fra.europa.eu/en/news/2020/how-concerned-are-europeans-about-their-personal-data-online
30 https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf
31 https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey#:~:text=Eighty%2Dthree%2-0percent%20of%20Australians,feel%20it%20is%20poorly%20protected.
32 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
33 https://fortune.com/2021/11/08/facebook-whistleblower-european-parliament-big-tech-eu/

7

Vie privée, consentement et réglementation des données

Les consommateurs étant de plus en plus informés sur la manière dont leurs données personnelles sont collectées, utilisées et détournées, ils exigent davantage de protections, de transparence, de confidentialité et de contrôle. En réponse, les gouvernements du monde entier ont rédigé et adopté une multitude de réglementations sur la vie privée :

Australie : Consumer Data Right (CDR) et l'amendement à la loi sur la protection de la vie privée (violations de données notifiables)

Bahreïn : Loi sur la protection des données personnelles

Brésil : La Lei Geral de Proteção de Dados (LGPD)

Canada : Digital Charter Implementation Act, pas encore adoptée

Chili : Loi sur la confidentialité des données, Ley 19,628

Chine : Loi sur la protection des données personnelles (PDPL), pas encore adoptée

Union européenne : Règlement Général sur la Protection des Données (RGPD)

Inde : Projet de loi sur la protection des données personnelles (PDPB), pas encore adopté

Kenya : Loi sur la protection des données

Qatar : Loi n°. 13

Afrique du Sud : Loi sur la protection des informations personnelles (POPIA)

Corée du Sud : Loi sur la protection des informations personnelles

Suisse : Loi sur la protection des données

Thaïlande : Loi sur la protection des données personnelles (PDPA)

États-Unis : Loi sur la protection de la vie privée des consommateurs de Californie (CCPA) et Loi sur les droits à la vie privée de Californie (CPRA)

États-Unis : Loi sur la protection de la vie privée du Colorado (CPA)

États-Unis : Loi SHIELD de New York

États-Unis : Loi de Virginie sur la protection des données des consommateurs (CDPA)

Turquie : Loi sur la protection des données personnelles n° 6698

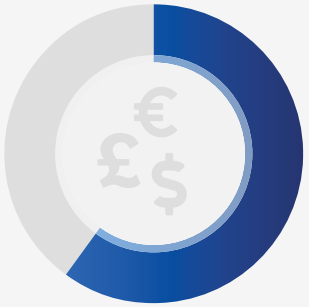
Bien qu'il existe des nuances, la majorité de ces règlementations exigent que les entreprises conservent les données en toute sécurité et informent les personnes en cas de faille de sécurité. Le RGPD, adopté en 2016, est la loi la plus complète et la plus approfondie. De nombreux gouvernements ont calqué leurs lois sur celle-ci. Le RGPD comprend des règles telles que :

- Le consentement pour l'utilisation des données personnelles doit être clairement accordé et facilement retiré.
- Toutes les données personnelles doivent être fournies au consommateur et supprimées sur demande.
- Les notifications de vols de données doivent être envoyées dans les 72 heures qui suivent la découverte d'un incident.
- La collecte et l'utilisation des données professionnelles doivent être conçues avec des protocoles de sécurité appropriés.

113,5%

Entre juillet 2020 et juillet 2021, le nombre de violations du Règlement Général sur la Protection des Données (RGPD) a augmenté de 113,5 %.[34]

L'importance d'adhérer aux réglementations liées à la protection de la vie privée n'échappe pas aux dirigeants d'entreprises. Entre juillet 2020 et juillet 2021, le nombre de violations du RGPD a augmenté de 113,5 %[35]. Pourtant, en 2021, Amazon a été condamné à verser une amende de 746 millions d'euros (888 millions de dollars) pour avoir enfreint le RGPD - la plus grosse amende jamais infligée.



Afin d'éviter les amendes et d'accroître la confiance des utilisateurs, 60 % des entreprises prévoient d'augmenter leurs dépenses en matière de protection de la vie privée en 2022.[36]

Les réglementations relatives aux données et à la vie privée devraient évoluer dans les années à venir, car les entreprises et la société continuent de négocier. Plusieurs pays discutent également de lois sur les ransomwares et d'une norme mondiale de protection de la vie privée.

Afin de renforcer la confiance des consommateurs, les entreprises doivent se conformer aux réglementations et laisser aux consommateurs le contrôle sur leurs données.

34, 35 https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
36 https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

8

Générations Z, Alpha et le métavers

On s'est beaucoup intéressé aux millennials (la génération Y) depuis un certain temps. Cependant, les grandes entreprises gardent un œil sur la génération Z (née entre 1997 et 2012) et sur la génération Alpha (née entre 2013 et 2028).

> La génération Z constituera bientôt le plus grand groupe de consommateurs. Les marques qui veulent profiter de cette opportunité devront comprendre leurs comportements et leurs attentes numériques.[37]
>
> INSIDER INTELLIGENCE

La génération Z est désormais la plus importante, constituant 32 % de la population mondiale et dépassant les millénials et les baby-boomers[38]. Cette génération exerce une forte influence sur les achats des ménages et son pouvoir d'achat annuel s'élève à 143 milliards de dollars.[39]

Ayant grandi à l'ère des ordinateurs personnels, des téléphones mobiles, des tablettes et d'une multitude de réseaux sociaux, les membres de la génération Z sont natifs du numérique.

143 Mrds $

La génération Z dispose actuellement d'un pouvoir d'achat de 143 milliards de dollars par an et exerce une forte influence sur les achats des ménages.[41]

Des recherches menées par WP Engine révèlent que 52 % des membres de la génération Z ne peuvent pas rester plus de quatre heures sans accès à internet sans se sentir mal à l'aise[40]. En outre, cette génération techniquement avisée ne fait pas de différence entre les canaux physiques et numériques.

La génération Z est suivie de la génération Alpha, les enfants de la génération Y. Les plus âgés de la génération Alpha ont moins de 10 ans, mais ils influencent plus de 500 milliards de dollars d'achats et sont dans l'attente de gratification instantanée.[42] Leurs jouets comprennent des objets connectés (IoT). Ils interagissent avec le monde par le biais de la réalité augmentée (AR) et de la réalité virtuelle (VR), et lorsqu'ils ont des questions, ils les posent à Alexa d'Amazon.

37 https://www.insiderintelligence.com/insights/generation-z-facts/
38 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/
39 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-spending-habits.html
40 https://wpengine.com.au/gen-z-aus/
41 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-spending-habits.html
42 https://www.spectrapartnership.com/shakeout-6-trends-shaping-generation-alpha-part-1/

8 Générations Z, Alpha et le métavers

La génération Z et la génération Alpha sont toutes deux fidèles aux expériences plutôt qu'aux marques. À cause de cela, de leur influence et de leurs prouesses numériques, les entreprises les plus ambitieuses surveillent de près ces deux générations et élaborent leurs plans de développement en conséquence. Cela inclut l'innovation des services et des produits de consommation au sein du métavers.

Si le concept de métavers existe depuis un certain temps, son développement n'en est qu'à ses débuts. Un métavers est une plateforme semblable à un jeu vidéo qui héberge des plateformes tierces dans lesquelles les utilisateurs peuvent entrer, sortir et interagir de manière fluide à l'aide d'une suite complète d'appareils connectés tels que des casques VR. Au cours de la prochaine décennie, les générations Z et Alpha ne se contenteront pas de jouer dans des métavers, elles y travailleront, y apprendront, y feront des achats et y investiront dans des objets et des biens immobiliers métavers dans le cadre de la préparation de leur retraite.[43]

Bien qu'elles soient encore jeunes, les générations Z et Alpha exercent une influence palpable sur les entreprises, la société et l'avenir. Le monde qu'ils revendiquent amplifie l'importance des huit tendances dont nous parlons.

43 https://www.wsj.com/articles/investors-see-promising-new-world-in-metaverse-11638455401

L'impératif CIAM

Sans aucun doute, les huit tendances décrites ci-dessus constituent une force dominante. Elles nécessitent que les entreprises soient capables de :

- Réinventer leurs stratégies commerciales et informatiques pour faire face à toute perturbation et répondre aux demandes évolutives des consommateurs avec agilité et résilience.
- Participer en toute sécurité à des écosystèmes numériques multipartites.
- Offrir aux clients des expériences multicanales sécurisées et fluides dans les environnements physiques et numériques.
- Sécuriser l'IoT et gérer les relations entre les personnes et leurs appareils.
- Respecter les réglementations relatives à la vie privée, au consentement et aux données et s'imposer comme des entreprises dignes de confiance.
- Identifier les risques et protéger contre la cybercriminalité et la fraude.
- Préparer l'avenir pour répondre aux besoins des générations futures.

Pour mener à bien ces objectifs, les entreprises les plus ambitieuses s'appuient sur une plateforme de CIAM (gestion des identités et des accès clients).

Le CIAM joue un rôle important en permettant aujourd'hui aux entreprises digitales d'acquérir et de fidéliser leurs clients, tout en leur fournissant les éléments de sécurité et de personnalisation nécessaires pour qu'ils s'engagent et effectuent des transactions avec l'entreprise.[44]

FORRESTER®

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

Quelles sont les réponses apportées par le CIAM ?

La gestion des identités et des accès clients (CIAM) est essentielle pour répondre à ces huit tendances. En d'autres termes, le CIAM apporte aux entreprises la possibilité de rassembler, de gérer et de sécuriser les identités et les données des clients et de l'IoT, de leur accorder le niveau d'accès approprié aux applications et aux services qu'ils recherchent et dont ils ont besoin, et de leur laisser le contrôle sur leurs paramètres de confidentialité et de partage de leurs données. Notre CIAM est spécialement conçu pour prendre en charge des milliards d'identités et pour offrir les fonctionnalités adaptées pour répondre aux tendances énumérées ici.

TENDANCES ET EXIGENCES	CAPACITÉS DU CIAM
1. L'économie de la réinvention Moderniser l'informatique pour faire face à toute perturbation et répondre aux demandes des consommateurs avec souplesse et résilience.	Pour soutenir la réinvention, une plateforme CIAM d'entreprise inclut les dernières technologies avec des fonctionnalités qui sont simples à mettre à jour et à modifier en un clin d'œil. La solution s'intègre également facilement sur site, dans le cloud ou dans un environnement hybride pour servir de point de référence unique pour la gestion des identités. Elle peut facilement évoluer pour prendre en charge des millions ou des milliards d'identités sans perturbations et sans add-ons tiers coûteux.
2. Écosystèmes partenaires La confiance entre les entreprises partenaires est nécessaire, comme la sécurité des intégrations et du partage des données.	Grâce au CIAM, les entreprises peuvent développer et étendre leurs activités avec de multiples partenaires en utilisant des intégrations préétablies (via les API REST) qui se connectent partout et sont nécessaires pour créer des expériences réussies. La solution sécurise les API et les points d'accès, inclut des solutions pré-intégrées de nos partenaires technologiques, et préserve la confidentialité et la sécurité des données.

TENDANCES ET EXIGENCES	CAPACITÉS DU CIAM
3. Expériences phygitales Offrir des expériences fluides dans les environnements physique et numérique.	Une solution CIAM permet aux entreprises d'offrir des expériences personnalisées et multicanales. Elle permet aux utilisateurs d'avoir une seule identité sur plusieurs appareils, en répondant à une multitude d'exigences techniques qui diffèrent selon les appareils, comme une montre-bracelet intelligente par rapport à une tablette ou un ordinateur portable. Le CIAM peut aussi rassembler les données issues de plusieurs systèmes pour fournir une vue unique sur l'utilisateur. À partir de cette vue unique, il est possible de créer des parcours personnalisés dans tous les environnements, qu'ils soient physiques ou numériques. Une solution CIAM simplifie également la manière dont les utilisateurs s'inscrivent, se connectent et gèrent leurs mots de passe et leurs paramètres pour une expérience optimale.
4. Internet des Objets (IoT) Nécessite la sécurité de l'identité IoT, la sécurité des données IoT et la capacité de gérer les relations entre les personnes et leurs objets connectés.	Une solution CIAM permet aux entreprises d'intégrer l'IoT dans leurs offres de produits avec le niveau de sécurité adéquat – car le niveau de sécurité requis pour une ampoule connectée est différent de celui d'un véhicule ou d'un réacteur nucléaire, bien sûr. La solution sécurise les données de l'IoT et les relie à l'identité d'une personne. Les entreprises peuvent utiliser la plateforme pour gérer les relations entre les objets IoT et les personnes qui les possèdent ou les utilisent.
5. Cybercriminalité, failles, fraudes… Exige que les entreprises identifient les risques et se protègent contre la cybercriminalité et la fraude.	La plateforme CIAM prend en charge des fonctionnalités et des modèles de sécurité avancés qui reposent sur le principe qu'il est impossible de faire confiance à une personne ou à un objet et qu'ils doivent être contrôlés en permanence. Le CIAM adopte les modèles de sécurité « Zero Trust », et CARTA (Continuous Adaptive Risk and Trust Assessment), qui permettent d'utiliser l'identité comme périmètre de sécurité pour analyser le risque d'accès en continu. Les entreprises peuvent également supprimer le besoin de mots de passe pendant le processus de connexion. Cette seule mesure permet d'éliminer les attaques par phishing, credential stuffing et de type man-in-the-middle lors des sessions. De plus, la solution comprend une architecture cloud qui isole les données de chaque organisation pour une sécurité optimale.

TENDANCES ET EXIGENCES	CAPACITÉS DU CIAM
6. Opinion publique et militantisme Instaurer la confiance et donner le contrôle aux utilisateurs	Grâce à une solution CIAM, les entreprises renforcent la confiance et la fidélité de leurs clients en leur donnant le contrôle sur leurs données et leurs paramètres, et en répondant à leurs demandes d'effacement de leurs données. De plus la solution contribue à préserver la réputation des entreprises grâce à ses fonctionnalités en matière de cybersécurité.
7. Vie privée, consentement et réglementation des données Il est nécessaire de respecter les réglementations en matière de confidentialité, de consentement et de données.	La plateforme CIAM permet aux entreprises de rester en conformité réglementaire grâce à des fonctionnalités qui donnent aux utilisateurs le contrôle sur leurs données, la confidentialité et leur consentement. Elle répond aussi aux exigences en matière de souveraineté et de résidence des données.
8. Générations Z, Alpha, et le métavers Tenir compte de toutes les tendances susmentionnées et faire preuve d'agilité pour en aborder de nouvelles.	Le CIAM permet aux entreprises de personnaliser les expériences et de créer des parcours clients en fonction de leurs préférences personnelles et générationnelles. La solution permet d'évoluer avec l'utilisateur et s'intègre facilement à d'autres technologies, nouvelles ou existantes.

Pourquoi les systèmes existants ou home-made sont inadéquats ?

Malheureusement, dans le but de réduire les coûts, de nombreuses entreprises ont tenté de modifier les systèmes existants de gestion des identités et des accès collaborateurs (IAM) pour répondre aux tendances et aux demandes, plutôt que d'investir dans une solution CIAM d'entreprise. Pourtant, comme l'a montré la disruption liée à la pandémie, les résultats sont loin d'être idéaux.

BMW a consolidé 20 systèmes existants différents pour la gestion des identités et des accès en une seule plateforme ForgeRock afin de réaliser d'importantes économies et d'améliorer le délai de mise sur le marché, l'évolutivité et la conformité.

Les systèmes IAM traditionnels sont conçus pour prendre en charge les cas d'utilisation touchant les collaborateurs ; ils ne sont pas conçus pour gérer des millions ou des milliards de clients, de partenaires et d'objets IoT - sans parler des données qui sont rassemblées. L'IAM traditionnel n'a pas non plus été conçu pour offrir des expériences multicanales faciles, ni pour prendre en charge des réglementations telles que le RGPD, ni pour atténuer les risques liés aux fraudes et à la cybercriminalité d'aujourd'hui.

De plus, les anciennes solutions IAM ne prennent pas en charge les normes modernes, ce qui rend plus difficile la connexion à ces solutions pour un écosystème de partenaires. Il est également très difficile et coûteux de les mettre à niveau, alors qu'elles doivent l'être pour répondre aux cas d'utilisation les plus fondamentaux d'aujourd'hui.

Plutôt que d'essayer de modifier l'IAM existant pour répondre aux tendances et se préparer à l'avenir, les entreprises doivent s'appuyer sur une plateforme CIAM spécialisée.

« ForgeRock nous permet, non seulement de transformer les parcours de nos clients aujourd'hui, mais aussi de disposer de la flexibilité nécessaire pour évoluer au fur et à mesure que le secteur se dirige vers un modèle plus écosystémique dans les années à venir. »

Chris Worle, Chief Digital Officer

HARGREAVES LANSDOWN

L’étude d’opportunité (ou le business case) du CIAM

Une solution de gestion des identités et des accès clients (CIAM) est le fondement de la réinvention, de la sécurité et de la disruption. Les plus grandes entreprises l’utilisent pour répondre à chacune des tendances évoquées tout en réduisant la charge sur leurs ressources informatiques. Grâce au CIAM, elles acquièrent des clients plus rapidement, offrent des expériences exceptionnelles à leurs clients et les protègent.

D’ici à 2025, les entreprises qui adoptent la gestion des identités et des accès clients (CIAM) avec détection convergente des fraudes et authentification sans mot de passe seront en mesure de réduire de plus de moitié leur taux d’attrition.[45]

Gartner®

45 https://www.gartner.com/en/documents/4009255-innovation-insight-for-customer-identity-and-access-management

1. Acquérir des clients plus rapidement

Une solution de CIAM contribue à accompagner les efforts de réinvention en intégrant les environnements sur site et dans le cloud dans l'informatique hybride - servant de source unique pour la gestion des identités dans l'ensemble de l'entreprise. De plus, le CIAM élimine les barrières entre les entreprises et leurs clients grâce à des processus d'inscription simplifiés et un profilage progressif. Le CIAM permet aussi aux entreprises d'instaurer la confiance et la fidélité en permettant aux clients de gérer facilement leurs mots de passe et leurs paramètres de confidentialité. Les entreprises peuvent développer des services à valeur ajoutée qui attirent les clients en participant en toute sécurité à des écosystèmes partenaires dynamiques. Tout cela se traduit par des **taux de conversion accélérés, des taux de rétention plus élevés et une plus grande fidélité des clients.**

2. Offrir des expériences exceptionnelles

Dans le cadre de leurs stratégies de réinvention, les entreprises doivent utiliser une solution de CIAM pour unifier des environnements hybrides disparates à travers l'entreprise. L'un des nombreux avantages obtenus est une vue unique du client, qui permet de personnaliser et d'adapter son parcours multicanal et phygital pour offrir des expériences vraiment exceptionnelles. Le CIAM permet également aux entreprises d'intégrer en toute sécurité l'IoT dans leurs offres et de participer à des écosystèmes numériques multipartites conçus pour offrir aux clients l'expérience fluide et pratique qu'ils attendent. La solution peut évoluer facilement en fonction de l'utilisation et de la demande sans perturbation pour les clients. Ces avantages, et bien d'autres encore, permettent d'**augmenter les recettes multicanales, de réduire le taux d'attrition et d'accroître la rentabilité à long terme.**

3. Protéger les clients

La réinvention passe par l'adoption d'une myriade de nouvelles technologies et par le test de nouvelles approches, comme la participation à des écosystèmes numériques de partenaires ou l'intégration de l'IoT dans les produits et services. Le CIAM est conçu pour sécuriser les utilisateurs, l'IoT et l'entreprise elle-même, ce qui permet d'intégrer en toute sécurité de nouvelles solutions dans les environnements informatiques.

Pour ce faire, notre CIAM prend pleinement en charge les modèles de sécurité avancés, comme le Zero Trust et CARTA, qui reposent sur le principe qu'il convient de contrôler en continu les personnes et les objets. Le CIAM est essentiel pour accompagner le respect des réglementations en matière de confidentialité, de consentement et de gestion des données. Un tableau de bord facile à utiliser est fourni pour contrôler les paramètres de confidentialité et de partage des données afin d'être assurés que l'entreprise se **conforme aux réglementations en matière de confidentialité et d'atténuer les risques et les fraudes.**

> « En avril 2020, nous avons lancé BBC Bitesize, un site Web qui fournit aux parents et aux étudiants des vidéos gratuites, des guides, des activités et des quiz par niveau et par sujet. Nous avons relancé le service en quelques semaines et nous avons eu trois millions d'utilisateurs le jour du lancement, sans aucun temps d'arrêt. »
>
> Matt Grest, Director of Platform
>
> BBC

ForgeRock : le leader incontesté du CIAM

En tant que leader incontesté du CIAM, ForgeRock accompagne efficacement les entreprises à aborder de front les nouvelles tendances de la transformation digitale. Avec ForgeRock, vous pouvez optimiser votre activité grâce à la seule plateforme complète du marché, , utilisant l'IA et conçue pour toutes les identités et tous les clouds.

Des entreprises internationales stimulent leur croissance et leurs résultats avec le CIAM de ForgeRock. Rejoignez la communauté ForgeRock et accompagnez vos initiatives spécifiques 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 de données et de consentement sur notre plateforme HealthSuiteDigital qui permettent de favoriser la confiance des clients et des patients. »

Jereon Tas, Chief Innovation and Strategy Officer

PHILIPS

Et maintenant ?

En savoir plus sur ForgeRock et le CIAM

- **Regardez** la vidéo de présentation du CIAM ForgeRock.
- **Découvrez** comment la BBC fournit un contenu personnalisé à plus de 45 millions d'utilisateurs dans le monde.
- **Téléchargez** notre guide de l'acheteur CIAM avec les caractéristiques essentielles, les définitions et les questions à poser aux éditeurs.

C'est le moment de migrer vers le cloud, d'exploiter l'intelligence artificielle et de profiter d'une infrastructure de nouvelle génération ; l'architecture que les entreprises construisent aujourd'hui déterminera leur avenir.[46]

accenture

Ressources indépendantes

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

- **The Forrester Wave™:** Gestion des identités et des accès des clients, 2022
- **Gartner®** Fonctionnalités stratégiques pour la gestion des accès, 2022
- **KuppingerCole Leadership Compass:** CIAM platforms, 2022

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

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

À propos de 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