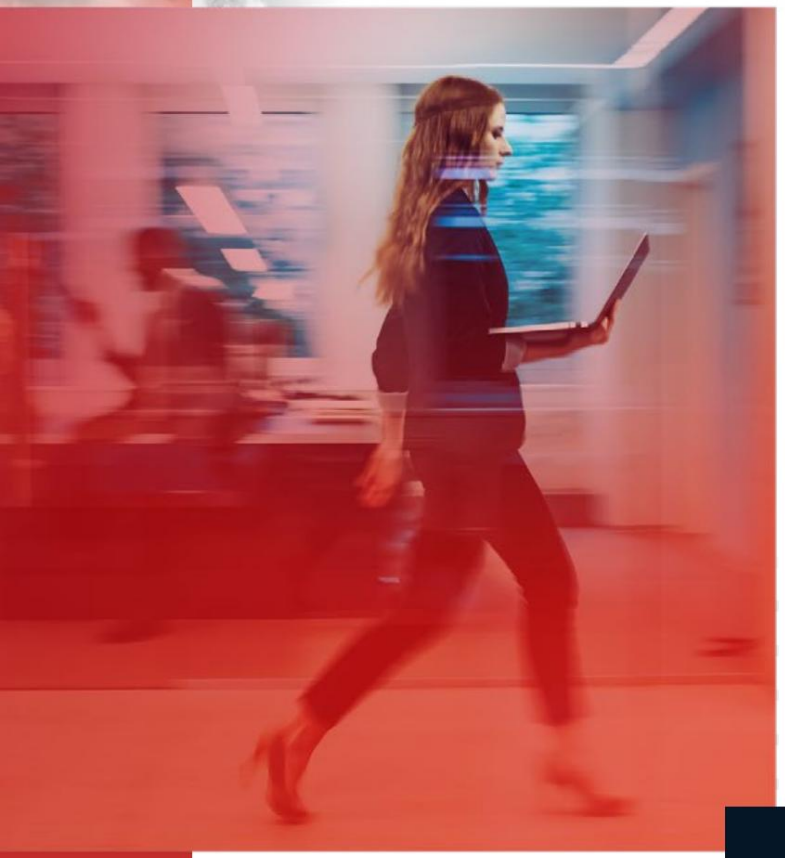


# Le 8 numérique Transformation

## Les tendances façonnent Affaires et Société

Pourquoi les tendances mondiales font de l'identité client et La gestion des accès (CIAM) est un impératif

# Résumé exécutif

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

## 1. Disrupted. L'économie de la réinvention

La pandémie a tout bouleversé. Aujourd'hui, les entreprises doivent se réinventer pour acquérir et fidéliser leurs clients, atténuer leurs pertes et assurer l'avenir de leurs activités.

## 2. Écosystèmes partenaires

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

## 3. Expériences phygitales

Peu importe comment et où les consommateurs interagissent avec une organisation, ils veulent une expérience transparente qui combine des 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 environ 188,34 milliards de dollars d'ici 2026.1
Malheureusement, la plupart des « choses » ne sont pas sécurisées.

## 5. Cybercriminalité, violations, fraudes et abus de pouvoir

Le nombre de violations de données, de fraudes, de ransomwares et de découvertes de dépassements de limites a explosé, sans aucun signe de ralentissement.

## 6. Opinion publique et activisme

Aujourd'hui, nous vivons à l'ère de la méfiance. L'opinion publique a adopté une attitude défensive. Les consommateurs veulent avoir le contrôle de leurs données personnelles et veulent que les organisations soient tenues responsables de leurs actes.

## 7. Réglementation sur la confidentialité, le consentement et les 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. D'autres réglementations sont attendues dans les années à venir.

## 8. La génération Z, la génération Alpha et le métavers

La génération Z est aujourd'hui la plus nombreuse, représentant 32 % de la population mondiale.2 Derrière elle, la génération Alpha a moins de 12 ans, mais ses membres influencent plus de 500 milliards de dollars d'achats. Dans les années à venir, la génération Z et la génération Alpha ne se contenteront pas de jouer dans les métavers, elles apprendront, travailleront, feront leurs achats et investiront également dans ces derniers.

Pour répondre aux huit tendances, les dirigeants d'entreprise se tournent vers des plateformes d'identité de niveau entreprise spécialement conçues pour les consommateurs, l'IoT et les cas d'utilisation prévus 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/

# Identité Ping : l'incontestable Chef du CIAM

Identifié comme le leader de l'identité externe et de la gestion des identités et des accès des consommateurs (CIAM) par Gartner, Forrester et KuppingerCole, ForgeRock Enterprise CIAM, désormais intégré à Ping Identity, est la seule solution du marché capable de répondre aux huit tendances et à l'avenir vers lequel elles pointent.

Ping Identity Enterprise CIAM permet aux entreprises de :

- Réinventer leurs stratégies commerciales et informatiques pour gérer toute perturbation et répondre aux demandes des consommateurs avec agilité et résilience à grande échelle
- Participer en toute sécurité à des écosystèmes numériques multipartites
- Offrir des expériences client omnicanales sécurisées et fluides dans les domaines physiques et numériques
- Sécuriser l'IoT et gérer les relations entre les personnes et leurs objets
- Adhérer aux réglementations en matière de confidentialité, de consentement et de données et s'établir comme des marques dignes de confiance
- Identifier et se protéger contre la cybercriminalité et la fraude
- Préparer leurs entreprises pour l'avenir afin de répondre aux demandes générationnelles

Avec Ping Identity, les entreprises peuvent non seulement répondre aux huit tendances, mais aussi les devancer. Les résultats de la solution CIAM de Ping Identity incluent de nouvelles opportunités de croissance des revenus grâce à des fonctionnalités conçues pour offrir des expériences client supérieures qui dépassent les attentes, une réduction des risques et de la fraude grâce à la sécurité Zero Trust, ainsi qu'une confiance et une fidélité numériques accrues grâce à une attention particulière portée à la confidentialité et au respect du consentement.

# Table des matières

# Les 8 transformations numériques Tendances qui façonnent les entreprises et la société

Pourquoi les tendances mondiales influencent-elles la clientèle ?

## Gestion des identités et des accès (CIAM) Un impératif

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

# 1 Perturbé.
# 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 omnicanales parfaites et personnalisées. Pour répondre à cette demande et garder une longueur d'avance sur la concurrence, les entreprises déploient d'énormes efforts pour innover en proposant de nouveaux services et peaufiner les expériences afin de « perturber » le marché.

**70% de** Les personnes interrogées ont estimé que la croissance disruptive était essentielle au succès de leur entreprise, mais seulement 13 % étaient convaincues que leur entreprise pouvait répondre à cette priorité stratégique.3

Deloitte.

Par exemple, en 2005, Amazon a bouleversé le marché avec Prime, en promettant une livraison gratuite en deux jours à ses membres. Plus de 15 ans plus tard, d'autres détaillants aspirent toujours à concurrencer cette attente désormais courante des consommateurs.

L'économie disruptive est par nature en constante évolution. Les entreprises développent de nouvelles façons innovantes de servir et de satisfaire leurs clients.
À leur tour, les consommateurs s'adaptent aux innovations et les transforment en attentes, incitant ainsi les entreprises à innover encore et encore.

La danse intime entre l'innovation numérique et les attentes des consommateurs oriente et façonne la société depuis plus de deux décennies. Avant la pandémie, la capacité à offrir des expériences client omnicanales irréprochables et personnalisées était à l'origine des initiatives de transformation numérique dans tous les secteurs. Pour la plupart des organisations, la planification et l'exécution de ces initiatives s'étalaient sur des années.
Cependant, lorsque la pandémie a frappé, les services numériques sont devenus une bouée de sauvetage pour les particuliers et les entreprises. En un instant, les délais de transformation numérique sont passés de quelques années à quelques semaines. Les entreprises qui en sont sorties gagnantes étaient celles qui disposaient déjà d'infrastructures informatiques modernisées et d'offres de services numériques capables de répondre à la demande des consommateurs dès le premier jour.

Avec la perturbation ultime provoquée par la pandémie, l'économie de la réinvention est née.

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

Partout dans le monde, la pandémie a déclenché une véritable tempête de transformation numérique. Aujourd'hui, alors que les entreprises et les gouvernements sont confrontés à l'incertitude économique mondiale, les dirigeants sont engagés dans une course pour acquérir et fidéliser les clients, atténuer leurs pertes et assurer l'avenir de leurs activités.

Pour être compétitives et servir les consommateurs dans un monde où le numérique est roi, les entreprises consacrent des ressources sans précédent à se réinventer pour devenir plus intelligentes, plus agiles et plus résilientes. Par exemple, elles restructurent leurs infrastructures informatiques et migrent vers le cloud lorsque cela est possible, intègrent des capteurs, des balises et des appareils IoT et mettent en œuvre l'intelligence artificielle.

83%

des dirigeants conviennent que les stratégies commerciales et technologiques de leur organisation deviennent indissociables, voire indissociables.4

accenture

(IA), apprentissage automatique (ML) et automatisation du traitement robotique (RPA) ; et création de jumeaux numériques et de mondes en miroir.

Alors que l'expérience client est au cœur de nos préoccupations, les efforts considérables déployés pour réinventer l'économie visent à préparer les entreprises à l'avenir, non seulement pour répondre aux besoins du monde actuel, mais aussi pour répondre à ceux du monde actuel. Pour cela, il faut associer stratégie commerciale et solutions technologiques modernes.

Il est essentiel d'acquérir des capacités prêtes pour l'avenir, en particulier pour bâtir une organisation résiliente, capable de détecter et de réagir à la volatilité et aux perturbations.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 : Accelerate Digital for Future-Ready Business. Cadres pour une technologie composable, des clients autonomes et l'avenir du travail, 2021

# 2 Écosystèmes partenaires

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

Selon McKinsey6, les écosystèmes numériques sont aujourd'hui au cœur de sept des douze plus grandes entreprises mondiales en termes de capitalisation boursière. Alimentés par 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, élargissent les offres de services et contribuent à offrir des expériences disruptives.

Par exemple, dans le secteur de la santé, les prestataires, les organismes payeurs, les détaillants et d'autres acteurs du secteur unissent leurs forces pour créer des écosystèmes de santé numériques qui combinent plusieurs services dans une seule application pratique destinée aux clients. Par exemple, avec une seule application, les consommateurs peuvent prendre rendez-vous, assister à des consultations de télésanté, consulter leurs résultats d'examen, payer leurs factures, soumettre une réclamation, recevoir des rappels et des conseils de soins et savoir quand leurs ordonnances sont prêtes à être récupérées.

Les grandes entreprises ont compris qu'unir leurs forces pour créer des solutions permettant une expérience client de bout en bout fluide est une stratégie gagnante. Les écosystèmes numériques multipartites s'appuient sur la sécurité des API et nécessitent d'accorder uniquement le niveau d'accès approprié aux systèmes et aux données au-delà des frontières organisationnelles.

## 60 000 milliards de dollars

Nos recherches montrent qu'un ensemble émergent d'écosystèmes numériques pourrait représenter plus de 60 000 milliards de dollars de revenus d'ici 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 -les-chances-de-l'écosystème-sont-vos-concurrents-le sont

# 3 expériences phygitales

La pandémie a eu de nombreux effets, notamment une nouvelle appréciation des expériences en personne. En même temps, elle a exposé le public aux avantages offerts par les services numériques.

Aujourd'hui, les gens recherchent le meilleur des deux mondes.

> À mesure que les entreprises réimaginent les possibilités offertes par les produits et services technologiques, elles découvriront bientôt qu'elles jouent un rôle plus actif que jamais auparavant dans la relation entre les personnes et la technologie.8
>
> accenture

Selon Ken Hughes, spécialiste des comportements des consommateurs et 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 de l'efficacité, mais la véritable connexion vient désormais du contact humain empathique. C'est une question de silicium et d'âme. »9

Le terme « omnicanal » désigne désormais tous les canaux, y compris le canal physique. Quelle que soit la manière dont les consommateurs interagissent avec une entreprise, ils souhaitent une expérience personnalisée et fluide qui reprend là où ils se sont arrêtés. Pour y parvenir, les entreprises conçoivent des expériences « phygitales » : des parcours clients personnalisés composés d'éléments physiques et numériques mixtes.

> Le physique + le numérique sont le nouveau sur-mesure. Au cours des 18 à 24 prochains mois, nous nous attendons à voir les entreprises leaders adopter la tendance du sur-mesure pour des milliards de personnes en explorant des moyens d'utiliser la conception centrée sur l'humain et la technologie numérique pour créer des interactions personnalisées et enrichies numériquement à grande échelle.10
>
> Deloitte.

Par exemple, certains prestataires de soins de santé utilisent des applications et la géolocalisation pour aider les patients à se déplacer dans les grands campus médicaux en leur fournissant des indications en temps réel pour se rendre à leur rendez-vous. Un autre exemple est celui des détaillants qui envoient des SMS aux clients lorsqu'ils sont dans le magasin physique, leur proposant des offres personnalisées ou même les invitant à trouver l'emplacement des produits qu'ils ont recherchés en ligne. Les restaurants proposent également des expériences phygitales en intégrant des codes QR qui lancent des menus. De plus, ils utilisent des applications qui permettent aux clients de diviser facilement leur addition et de payer leurs factures. Les expériences phygitales ont également fait leur chemin dans les magasins de vêtements. Certains détaillants, comme Macy's, ont installé des miroirs intelligents à réalité augmentée (AR) dans leurs magasins physiques, qui permettent aux clients de voir à quoi ressemblent les vêtements sur eux avant de les essayer physiquement.

Dans les années à venir, l'intégration des expériences numériques et physiques occupera une place prépondérante dans la vie quotidienne. Il est important de noter que pour offrir des expériences phygitales, il faut connaître le client à chaque point de contact et garantir la sécurité et la confiance.

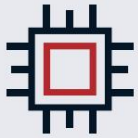
8 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Rapport-complet.pdf

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 appareils intelligents et le Internet des objets

Les appareils intelligents constituant l'Internet des objets (IoT) sont devenus omniprésents à mesure que les organisations de tous les secteurs innovent en proposant de nouvelles offres et expériences phygitales. Selon Market Data Forecast,11 le marché mondial de l'IoT grand public devrait passer de 97,50 milliards de dollars en 2020 à environ 188,34 milliards de dollars d'ici 2026.



Les appareils de l'Internet des objets (IoT) font partie des 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 entreprises axées sur le consommateur s'appuient de plus en plus sur les objets IoT, les données qu'ils collectent et les applications auxquelles ils se connectent. à.

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

Alors que l'IoT améliore la vie des consommateurs et aide les organisations à se différencier avec de nouvelles offres de services, la triste réalité est que la plupart des objets IoT ne sont pas sécurisés et peuvent être utilisés de manière malveillante. Les cyberattaques IoT ont plus que doublé d'une année sur l'autre au cours du premier semestre 2021, entraînant quelque 1,51 milliard de violations, contre 639 millions en 2020.13

Il est important de noter que les conséquences des piratages et des violations de l'IoT peuvent être désastreuses, ce qui fait de la sécurité des identités IoT et de leurs données 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, violations, fraudes et abus de pouvoir

L'essor du numérique s'accompagne d'une évolution des tactiques de cybercriminalité et de cyberguerre. Aujourd'hui, rien n'est plus grave pour une entreprise qu'un piratage, une violation ou une réputation ternie en raison de mauvaises pratiques de sécurité et de gestion des données.

Au cours des dernières années seulement, le nombre de violations, d'attaques de phishing, de fraudes, de ransomwares et de dépassements de sécurité a atteint de nouveaux sommets.

La croissance attendue des appareils intelligents, de la 5G, de l'informatique de pointe et de l'intelligence artificielle promet de créer encore plus de données, de nœuds connectés et de surfaces d'attaque étendues.14

Deloitte.

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

**80%** Les applications Web constituent le principal vecteur d'attaque, liées à plus de 80 % des violations.16

**61%** 61 % de toutes les violations de données sont le résultat de stratagèmes, tels que le phishing, qui volent les identifiants de connexion.17

**2B** 2 milliards d'enregistrements de données contenant des noms d'utilisateur et des mots de passe ont été compromis en 2021.18

**136%** Les cyberattaques IoT ont augmenté de 136 % au cours du seul premier semestre 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 communes utilisées pour accéder à un système informatique (noms d'utilisateur, mots de passe et informations personnelles identifiables) font partie des formes d'informations les plus convoitées par les cybercriminels.

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

Bien que des progrès aient été réalisés ces dernières années, les répercussions juridiques des violations et des abus ne sont souvent pas à la hauteur des attentes des consommateurs. De plus, lorsque des informations personnelles ont été volées, les consommateurs sont très insatisfaits des compensations et des réparations qui leur sont offertes par les organisations.

Le public est désillusionné. Plus d'une décennie de violations de données qui ont fait l'actualité a eu un impact non seulement sur la façon dont les gens perçoivent et interagissent avec les organisations, mais aussi sur ce qu'ils attendent en termes de sécurité, d'accès, de contrôle et d'utilisation de leurs données personnelles.

Lorsque ces responsabilités « B to C bidirectionnelles » ne sont pas respectées, les résultats sont pires que des clients déçus : l'échec crée une société désillusionnée par le modèle d'innovation intégré sur lequel les entreprises s'appuient 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 activisme

La société a atteint un âge de méfiance. Dans ce contexte, les gens sont parfaitement conscients des capacités de collecte de données des moteurs de recherche, des cookies et des objets connectés, ainsi que de la menace de la cybercriminalité, comme le phishing et la fraude. 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 des données personnelles avec une organisation sont la collecte et le stockage sécurisés (63 %), suivis du contrôle sur les données partagées (57 %) et de la confiance dans l'entreprise (51 %). Si ces garanties ne sont pas fournies par les organisations, ils les chercheront ailleurs.25

EY

Selon plusieurs enquêtes menées par des organisations telles que Pew Research Center, l'Agence de l'Union européenne pour les droits fondamentaux Droits, EY, PwC, Salesforce et RSA :

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

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

**81%** des consommateurs déclarent que les risques potentiels auxquels ils sont confrontés du fait de la collecte de données par les entreprises dépassent 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/
29 https://fra.europa.eu/en/news/2020/how-concerned-are-europeans-about-their-personal-data-online

41%

des résidents de l'Union européenne ne souhaitent pas partager de données personnelles avec des entreprises privées.29

64%

des Américains blâment l'entreprise, et non le pirate informatique, lorsque leurs données sont piratées.30

83%

des Australiens souhaiteraient que le gouvernement fasse davantage pour protéger la confidentialité de leurs données.31

Comme le montrent les statistiques ci-dessus, l'opinion publique a adopté une attitude défensive, ce qui rend l'interaction entre les entreprises et la société très importante. En conséquence, la société est désormais le moteur de la transparence organisationnelle et de l'élaboration de réglementations.

Par exemple, Max Schrems, avocat militant, a lancé des campagnes contre Facebook, désormais appelé Meta Inc., pour violation de la vie privée et inadéquation du cadre du Privacy Shield de l'Union européenne (UE) et des États-Unis. La Cour de justice de l'Union européenne (CJUE) a statué en faveur de Schrems dans deux affaires, modifiant la manière dont les organisations traitent les données des utilisateurs à l'échelle mondiale.

La confiance et l'adoption iront de pair pour la prochaine génération de produits et de services.32

accenture

Un autre exemple est le témoignage de la lanceuse d'alerte de Facebook, Frances Haugen, qui a révélé que l'entreprise n'avait pas donné suite à une étude montrant que les algorithmes et les tactiques utilisés sur les plateformes Instagram et Facebook sont nocifs pour les jeunes filles et les adolescentes, entre autres révélations clés. Ce témoignage a suscité un soutien bipartisan aux États-Unis en faveur d'une action réglementaire. Il donne également un élan au projet de loi sur les services numériques (DSA) de l'UE, qui vise à limiter strictement les contenus illégaux, y compris la désinformation, et à contraindre l'industrie de la haute technologie à rendre plus transparents les algorithmes qui collectent les données personnelles des personnes et ciblent les contenus pour les utilisateurs.33

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-australi an-community-attitudes-to-privacy-survey#:~:text=Quatre-vingts%2Dtrois%20percent%20of%20Australiens, se sentent%20it%20is%20mal%20protégés.

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 Confidentialité, consentement et données

## Règlements

Les consommateurs étant mieux informés sur la manière dont leurs données personnelles sont collectées, utilisées et détournées, ils exigent davantage de protection, de transparence, de confidentialité et de contrôle. En réponse, les gouvernements du monde entier ont élaboré et adopté une multitude de réglementations sur la confidentialité.
Il s'agit notamment de :

Australie : Droit aux données des consommateurs (CDR) et
Modification de la loi sur la protection des renseignements personnels (violations de données à déclaration obligatoire)

Bahreïn : loi sur la protection des données personnelles

Brésil : Lei Geral de Proteçao de Dados (LGPD)

Canada : Loi de mise en œuvre de la Charte du numérique (pas encore adoptée)

Chili : loi sur la protection des données, Ley 19,628

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

Union européenne : Protection générale des données Règlement (RGPD)

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

Israël : réglementation sur la sécurité des données

Japon : loi sur la protection des données personnelles

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 données personnelles

Suisse : Loi sur la protection des données

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

États-Unis : California Consumer Privacy Act (CCPA) et California Privacy Rights Act (CPRA)

États-Unis : Colorado Privacy Act (CPA)

États-Unis : Loi SHIELD de New York

États-Unis : Virginia Consumer Data Protection Act (CDPA)

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

Bien qu'il existe des nuances, la majorité de ces réglementations exigent que les organisations protègent les données et avertissent les personnes en cas de violation. Le RGPD, adopté en 2016, est la réglementation la plus complète et la plus approfondie. De nombreux autres gouvernements ont calqué leurs lois sur lui. Le RGPD comprend des règles telles que :

- Le consentement à l'utilisation des données personnelles doit être clairement accordé et facilement retiré.
- Toutes les données personnelles doivent être fournies au consommateur et supprimées (effacé) sur demande.
- Les notifications de violation doivent être envoyées dans les 72 heures suivant la découverte d'un incident.
- La collecte et l'utilisation des données organisationnelles doivent être conçues en tenant compte 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

Les dirigeants d'entreprise sont conscients de l'importance de respecter les obligations en matière de protection de la vie privée. Entre juillet 2020 et juillet 2021, le nombre de violations du RGPD a augmenté de 113,5 %.35 Par exemple, en 2021, Amazon a été condamnée à une amende de 746 millions d'euros (888 millions de dollars) pour violation du RGPD, soit la plus grosse amende jamais infligée.

Pour éviter les amendes et accroître la confiance des utilisateurs, 60 % des organisations prévoient d'augmenter leurs dépenses liées à la confidentialité en 2022.36

Les réglementations en matière de données et de confidentialité devraient évoluer dans les années à venir, à mesure que les entreprises et la société continuent de négocier. Plusieurs pays discutent également de lois sur les ransomwares et d'une norme mondiale de confidentialité.

Afin de préserver et de renforcer la confiance des consommateurs, les entreprises doivent se conformer aux réglementations et donner aux consommateurs le contrôle de 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 Génération Z, Génération Alpha et le métavers

Les Millennials font la une des journaux depuis un certain temps déjà. Mais les grandes entreprises ont également les yeux rivés sur les futurs créateurs de la génération Z (nés entre 1997 et 2012) et de la génération Alpha (nés entre 2013 et 2028).

> La génération Z deviendra bientôt la plus grande cohorte de consommateurs – et les marques qui veulent profiter de cette opportunité devront comprendre leurs tendances et leurs attentes numériques.34
>
> INSIDER INTELLIGENCE

La génération Z est désormais la plus nombreuse, constituant 32 % de la population mondiale et surpassant les millennials et les baby-boomers.38 Cette génération a une forte influence sur les achats des ménages et son pouvoir d'achat annuel est de 143 milliards de dollars.39

## 143 milliards de dollars

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

Ayant grandi à l'ère des ordinateurs personnels, des téléphones portables, des tablettes et d'une multitude de plateformes de médias sociaux, la génération Z est une native du numérique. Une étude menée par WP Engine révèle que 52 % des membres de la génération Z ne peuvent pas rester plus de quatre heures sans accès à Internet avant de se sentir mal à l'aise.40 De plus, cette génération techniquement experte ne fait pas la différence entre les canaux physiques et numériques. Et, alors que les Millennials sont ravis d'expériences instantanées, fluides, prédictives et personnalisées 24 heures sur 24, 7 jours sur 7, la génération Z ne tolérera rien de moins. Ils sont également plus protecteurs de leurs informations personnelles en raison du fait qu'ils ont grandi au milieu de violations très médiatisées.

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-sending-habits.html
40 https://wpengine.com.au/gen-z-aus/
41 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-sending-habits.html
42 https://www.spectrapartnership.com/shakeout-6-trends-shaping-Generation-alpha-part-1/

La génération Z est suivie par la génération Alpha, les enfants de la génération Y. Les aînés de la génération Alpha ont moins de 12 ans, mais ils influencent plus de 500 milliards de dollars d'achats et sont programmés pour la gratification instantanée.42 Leurs jouets incluent des objets connectés IoT. Ils interagissent avec le monde grâce à la réalité augmentée (AR) et à la réalité virtuelle (VR).

Et quand ils ont des questions, ils demandent à Alexa d'Amazon
réponses.

La génération Z et la génération Alpha sont toutes deux plus fidèles aux expériences qu'aux marques. Grâce à cela, à leur influence et à leurs prouesses numériques, les grandes entreprises sont à l'écoute de la génération Z et de la génération Alpha et élaborent leurs feuilles de route de produits en conséquence. Cela inclut l'innovation en matière de services et d'objets grand public au sein des métavers.

Bien que le concept de métavers existe depuis un certain temps, son développement n'en est qu'à ses balbutiements.
Le métavers est une plateforme de type jeu vidéo qui héberge des plateformes tierces permettant aux utilisateurs d'entrer, de sortir et d'interagir de manière transparente à l'aide d'une suite complète d'appareils connectés tels que des casques de réalité virtuelle. Au cours de la prochaine décennie, la génération Z et la génération Alpha ne se contenteront pas de jouer dans les métavers, ils apprendront, travailleront, feront des achats et investiront également dans ceux-ci.43

Bien qu'elles soient encore jeunes, les générations Z et Alpha ont une influence tangible sur les entreprises, la société et l'avenir. Le monde qu'elles contribuent à façonner amplifie l'importance de ces huit tendances.

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

# L'impératif du CIAM

Il ne fait aucun doute que les huit tendances décrites ci-dessus constituent une force dominante. Elles nécessitent que les organisations soient capables de :

- Réinventer leurs stratégies commerciales et informatiques pour gérer toute perturbation et répondre aux demandes des consommateurs avec agilité et résilience à grande échelle
- Participer en toute sécurité à des écosystèmes numériques multipartites
- Offrir des expériences client omnicanales sécurisées et fluides dans les domaines physique et numérique
- Sécuriser l'IoT et gérer les relations entre les personnes et leurs affaires
- Respecter les réglementations en matière de confidentialité, de consentement et de données et établir elles-mêmes comme des marques dignes de confiance
- Identifier et se protéger contre la cybercriminalité et la fraude
- Préparer leurs entreprises pour l'avenir afin de répondre aux demandes générationnelles

Pour atteindre tous les objectifs ci-dessus, les grandes entreprises s'appuient sur une plateforme CIAM de niveau professionnel.

Le CIAM joue un rôle important en aidant les entreprises numériques d'aujourd'hui à acquérir et à fidéliser leurs clients, tout en leur fournissant les fonctionnalités de sécurité et de personnalisation nécessaires pour qu'elles puissent s'engager et effectuer 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

# Comment répondre aux huit tendances avec Enterprise CIAM

La gestion des identités et des accès des consommateurs (CIAM) est essentielle pour répondre aux huit tendances. En termes simples, la CIAM permet aux organisations de collecter, de gérer et de sécuriser les identités et les données des consommateurs et de l'IoT, d'accorder aux consommateurs et à l'IoT le niveau d'accès approprié aux applications et aux services, et de donner aux consommateurs le contrôle de leurs paramètres de confidentialité et de partage de données. La CIAM d'entreprise est spécialement conçue pour prendre en charge des milliards d'identités et pour fournir les fonctionnalités énumérées ci-dessus à l'échelle d'Internet.

Le tableau suivant répertorie chaque tendance et la manière dont le CIAM de niveau entreprise les aborde.

| TENDANCE ET EXIGENCE | CAPACITÉ CIAM |
|---|---|
| **1. L'économie de la réinvention**<br>Nécessite une modernisation informatique pour gérer toute perturbation et répondre aux demandes des consommateurs avec agilité et résilience | Pour soutenir la réinvention, une plateforme CIAM d'entreprise comprend les dernières technologies avec des fonctionnalités simples à mettre à jour et à modifier à tout moment. La solution CIAM d'entreprise s'intègre également facilement aux environnements hérités et cloud de l'informatique hybride pour servir de point de vérité unique pour l'identité. Et elle peut facilement évoluer pour prendre en charge des millions ou des milliards d'identités sans ajouts tiers coûteux ni interruption. Il est important de noter que la solution CIAM de niveau entreprise est simple à mettre à jour. |
| **2. Écosystèmes partenaires**<br>Nécessite une confiance entre les organisations partenaires, en plus d'intégrations sécurisées et de partage de données | Avec Enterprise CIAM, les entreprises peuvent développer et étendre leurs activités avec plusieurs partenaires à l'aide d'intégrations prédéfinies (via les fonctionnalités REST API) qui se connectent partout et sont nécessaires pour créer des expériences exceptionnelles. Enterprise CIAM sécurise également les API et les points d'accès, inclut des solutions de partenaires technologiques pré-intégrées et préserve la confidentialité et la sécurité des données. |
| **3. Expériences phygitales**<br>Nécessite de proposer des expériences fluides dans les domaines physique et numérique | Une plateforme CIAM d'entreprise permet aux entreprises de proposer des expériences personnalisées et omnicanales. Elle permet aux utilisateurs d'avoir une identité unique sur plusieurs appareils en répondant à une multitude d'exigences techniques qui diffèrent selon les appareils, comme une montre connectée par rapport à une tablette ou un ordinateur portable. La plateforme CIAM d'entreprise peut également combiner des données provenant de plusieurs systèmes pour fournir une vue unique du consommateur. À partir de cette vue unique, ils peuvent créer des parcours client personnalisés dans des environnements physiques et numériques.<br>Enterprise CIAM simplifie également la manière dont les utilisateurs s'inscrivent, se connectent et gèrent leurs mots de passe et paramètres pour une expérience exceptionnelle. |

| TENDANCE ET EXIGENCE | CAPACITÉ CIAM |
|---|---|
| 4. Les appareils intelligents et l'Internet des objets nécessitent la sécurité de l'identité IoT, la sécurité des données IoT et la capacité de gérer les relations entre les personnes et leurs objets | Une plateforme CIAM d'entreprise permet aux organisations d'intégrer l'IoT dans leurs offres de produits avec le niveau de sécurité approprié. Par exemple, le niveau de sécurité requis pour une ampoule connectée est différent de celui d'un véhicule ou d'un réacteur nucléaire.<br>Enterprise CIAM permet également de sécuriser les données IoT et peut les lier à l'identité d'une personne.<br>Les organisations peuvent également utiliser une plateforme CIAM pour gérer les relations entre les objets IoT et les personnes qui les possèdent ou les utilisent. |
| 5. Cybercriminalité, violations, fraudes et abus de pouvoir Les organisations doivent identifier et se protéger contre la cybercriminalité et la fraude. | Les plateformes CIAM d'entreprise prennent en charge des fonctionnalités et des modèles de sécurité avancés qui reposent sur le principe selon lequel aucune personne ni aucun objet ne peut être digne de confiance et doivent être constamment vérifiés. Les plateformes CIAM d'entreprise permettent ce que l'on appelle un modèle de sécurité Zero Trust, ou évaluation continue adaptative des risques et de la confiance (CARTA), qui permet d'utiliser l'identité comme périmètre de sécurité pour analyser le risque d'accès de manière continue.<br>Les entreprises peuvent également supprimer le besoin de mots de passe lors du processus de connexion. Cela permet d'éliminer les attaques de phishing, le vol d'identifiants et les attaques de l'homme du milieu sur les sessions. En outre, le CIAM d'entreprise comprend une architecture cloud qui isole les données de chaque entreprise pour une sécurité optimale. |
| 6. L'opinion publique et l'activisme nécessitent d'instaurer la confiance et de donner le contrôle aux consommateurs | Grâce au CIAM d'entreprise, les entreprises peuvent renforcer la confiance et la fidélité en donnant aux clients le contrôle de leurs données et de leurs paramètres, ainsi qu'en honorant leurs demandes d'effacement de leurs données. De plus, comme indiqué ci-dessous, le CIAM d'entreprise contribue à préserver la réputation des organisations grâce à ses vastes capacités de cybersécurité. |
| 7. Réglementations sur la confidentialité, le consentement et les données Nécessite le respect des réglementations sur la confidentialité, le consentement et les données | Les plateformes CIAM d'entreprise aident les organisations à respecter les obligations réglementaires grâce à des fonctionnalités qui permettent aux consommateurs de contrôler les données, la confidentialité et le consentement. Elles contribuent également à répondre aux exigences de souveraineté et de résidence des données. |
| 8. Génération Z, génération Alpha et le métavers<br><br>Nécessite de prendre en compte toutes les tendances ci-dessus ainsi que l'agilité nécessaire pour en aborder de nouvelles | Enterprise CIAM permet aux entreprises de personnaliser les expériences et de créer des parcours clients en fonction des préférences personnelles et générationnelles. Il peut également évoluer avec le consommateur, en commençant par lui en tant qu'enfant ou personne à charge du compte de ses parents, puis en le faisant passer à son propre compte lorsqu'il vieillit. De plus, il s'intègre facilement à d'autres technologies, nouvelles et anciennes. |

# Pourquoi Legacy et Homegrown Les systèmes d'identité sont inadéquats

Malheureusement, dans un effort de réduction des coûts, de nombreuses organisations ont essayé de modifier leurs systèmes IAM actuels pour répondre aux tendances et aux demandes, plutôt que d'investir dans une solution CIAM d'entreprise. Pourtant, comme l'ont montré les perturbations causées par la pandémie, les résultats sont loin d'être idéaux.

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

Les systèmes IAM traditionnels sont conçus pour prendre en charge les cas d'utilisation des employés ; ils ne sont pas conçus pour gérer des millions ou des milliards de clients, de partenaires et d'objets IoT, sans parler des données qu'ils accumulent. Les solutions IAM traditionnelles n'ont pas non plus été conçues pour offrir des expériences omnicanales sans effort, ni pour prendre en charge des réglementations telles que le RGPD, le CCPA ou le CDR, ni pour atténuer le risque de cybercriminalité et de fraude sophistiquées d'aujourd'hui. De plus, les solutions IAM traditionnelles ne prennent pas en charge les solutions modernes

Les normes sont de plus en plus strictes, ce qui rend plus difficile la connexion d'un écosystème de partenaires à ces normes. Il est également très difficile et coûteux de les mettre à niveau, mais elles doivent l'être pour répondre aux cas d'utilisation les plus élémentaires d'aujourd'hui, sans parler des huit tendances.

Plutôt que d'essayer de modifier l'IAM existant pour répondre aux huit tendances et se préparer à l'avenir, les organisations doivent tirer parti d'une plate-forme CIAM spécialement conçue pour l'entreprise.

« ForgeRock nous permet non seulement de transformer le parcours de nos clients aujourd'hui, mais également d'avoir la flexibilité nécessaire pour évoluer à mesure que l'industrie évolue vers un modèle davantage écosystémique dans les années à venir. »

Chris Worle, directeur numérique

HARGREAVES LANSDOWN

# L'argument commercial en faveur de

# Entreprise CIAM

Une plateforme CIAM d'entreprise est la base de la réinvention, de la sécurité et de la disruption. Les grandes entreprises l'utilisent pour répondre à chacune des huit tendances tout en réduisant la charge pesant sur leurs ressources informatiques. Avec le CIAM d'entreprise, ils acquièrent des clients plus rapidement, offrent d'excellentes expériences et protègent leurs clients.

D'ici 2025, les organisations qui adopteront 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 le taux de désabonnement des clients de plus de moitié.45

Gartner

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

## 1. Acquérir des clients plus rapidement

Les plates-formes CIAM modernes contribuent à soutenir les efforts de réinvention en intégrant les environnements hérités et cloud dans l'ensemble de l'informatique hybride, servant ainsi de source unique de vérité pour l'identité dans toute l'entreprise. De plus, les fonctionnalités CIAM d'entreprise éliminent les barrières entre les organisations et leurs clients grâce à des fonctionnalités telles qu'un processus d'enregistrement simple et un profilage progressif. Le CIAM aide également les organisations à instaurer la confiance et la fidélité en permettant aux consommateurs de gérer facilement leurs mots de passe et leurs paramètres de confidentialité. De plus, avec le CIAM d'entreprise, les organisations peuvent développer des services à valeur ajoutée qui attirent les clients en participant en toute sécurité à des écosystèmes de partenaires numériques dynamiques. Tout cela se traduit par des taux de conversion accélérés, des taux de rétention plus élevés et une plus grande fidélité des clients. En fait, selon une étude de Forrester Consulting Total Economic Impact™ (TEI)
Étude : les entreprises ont augmenté les taux de conversion des clients de 133 % sur trois ans avec ForgeRock CIAM.46

## 2. Offrez des expériences exceptionnelles

Dans le cadre de leurs stratégies de réinvention, les entreprises peuvent utiliser le CIAM d'entreprise pour unifier des environnements hybrides disparates au sein de l'entreprise. L'un des nombreux avantages est une vue unique du client, qui permet aux entreprises de personnaliser les parcours utilisateur omnicanaux et phygitaux pour offrir des expériences exceptionnelles.
Enterprise 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 les expériences simples et pratiques qu'ils souhaitent. Il peut également évoluer facilement en fonction de l'utilisation et de la demande sans perturber les clients. Ces avantages et bien d'autres conduisent à des revenus omnicanaux plus élevés, à une baisse du taux de désabonnement des clients et à une meilleure rentabilité à long terme. Selon l'étude TEI de Forrester, les entreprises ont enregistré une amélioration de 400 % des taux d'engagement sur trois ans avec ForgeRock CIAM.47

## 3. Protégez vos clients

La réinvention comprend l'adoption d'une myriade de nouvelles technologies et l'essai de nouvelles approches, telles que la participation à des écosystèmes de partenaires numériques ou l'intégration de l'IoT dans des produits et services. Enterprise CIAM est spécialement conçu pour sécuriser les consommateurs, l'IoT et l'entreprise, permettant ainsi aux organisations d'intégrer en toute sécurité de nouvelles solutions dans leurs stratégies commerciales et leurs environnements informatiques. Enterprise CIAM y parvient en prenant entièrement en charge des modèles de sécurité avancés, tels que Zero Trust et CARTA, qui reposent sur le principe selon lequel aucune personne ou aucun objet ne peut être digne de confiance et doivent être constamment vérifiés.
Enterprise CIAM est également essentiel pour respecter les réglementations en matière de confidentialité, de consentement et de données. Il fournit aux clients un tableau de bord facile à utiliser pour contrôler leurs paramètres de confidentialité et de partage de données. Tout cela aide les organisations à se conformer aux réglementations en matière de confidentialité et à atténuer les risques et la fraude. Forrester rapporte que les clients ForgeRock CIAM ont réduit de 40 % les appels liés à la sécurité au centre d'appels et ont diminué l'impact de la fraude, ce qui a permis d'économiser 4,7 millions de dollars.48

Lisez l'étude Forrester Total Economic Impact™ sur la gestion des identités et des accès des clients de ForgeRock pour découvrir comment les entreprises ont obtenu un retour sur investissement (ROI) de 186 %.

FORRESTER®

46, 47, 48 https://www.forgerock.com/resources/analyst-report/186-roi-new-total-economic-impacttm-study

# Identité Ping : l'incontestable Responsable CIAM d'entreprise

En tant que leader incontesté du CIAM, Ping Identity aide les entreprises à aborder de front les huit tendances de la transformation numérique.
Avec Ping Identity, vous pouvez faire de meilleures affaires avec la seule plate-forme professionnelle du secteur, complète et pilotée par l'IA, spécialement conçue pour toutes les identités et tous les cloud.

Les entreprises internationales stimulent leur croissance et leurs revenus grâce à Ping Identity CIAM. Rejoignez la communauté Ping et soutenez vos initiatives de réinvention uniques pour répondre non seulement aux tendances d'aujourd'hui, mais aussi à celles de demain.

FORRESTER®

CHEF

Forrester Wave™
Identité du client et
Gestion des accès,
4e trimestre 2022

Gartner

SCORE LE PLUS ÉLEVÉ

Gartner® Critical
Capacités pour l'externe
Gestion des accès et
des applications
Développement, 2022

kuppingercole ANALYSTS

LEADER GÉNÉRAL

Kuppinger Cole
Boussole de leadership,
Plateformes CIAM, 2022

« Chez Philips, nous avons pour mission d'améliorer la vie des gens et de leur permettre 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 au sein de notre plateforme HealthSuiteDigital, qui permettent de renforcer la confiance des consommateurs et des patients. »

Jereon Tas, directeur de l'innovation et de la stratégie

PHILIPS

# Où aller à partir d'ici

## En savoir plus sur Ping Identity et CIAM

- Montre la vidéo de présentation de Ping Identity CIAM
- Lire Comment la BBC propose un contenu personnalisé à plus de 45 millions d'utilisateurs dans le monde
- Télécharger notre guide d'achat CIAM qui comprend les fonctionnalités essentielles, les définitions d'identité et les questions d'appel d'offres à poser aux fournisseurs

Il est désormais temps de migrer vers le cloud, d'exploiter l'IA et de tirer parti de l'infrastructure de nouvelle génération ; l'architecture que les entreprises construisent aujourd'hui déterminera leur avenir.49

accenture

## Tierce partie indépendante Ressources

Consultez le placement des points et lisez ces rapports d'analystes pour découvrir pourquoi Ping Identity est le leader du CIAM d'entreprise :

- Étude Forrester Total Economic Impact™ sur Identité et accès client ForgeRock Gestion
- La vague Forrester™ : Identité et accès client Gestion, 2022
- Gartner® Capacités critiques pour la gestion des accès, 2022
- Boussole de leadership KuppingerCole : Plateformes CIAM, 2022

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

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