

Libérer le potentiel de l'identité numérique dans le secteur financier



Optimiser la transformation digitale, accélérer l'adoption de la banque numérique et moderniser l'écosystème des services financiers connectés.

Introduction	2
Libérer le potentiel de l'identité numérique dans les services financiers	3
Optimiser la transformation digitale	5
Accélérer l'adoption de la banque numérique	8
Moderniser l'écosystème des services financiers connectés	11
Conclusion	13

Introduction

Vous avez conscience des forces qui poussent au changement dans les services financiers. L'émergence de technologies disruptives, l'importance croissante des fournisseurs tiers de confiance (TTP) et l'expansion de l'écosystème des services financiers sont en train de déloger les modèles traditionnels et d'estomper les frontières concurrentielles. Les clients exigent plus de contrôle, un meilleur accès et une personnalisation omnicanale. Les fournisseurs adoptent de nouvelles façons de penser et augmentent leurs investissements dans des offres à valeur ajoutée. Dans de nombreuses régions du monde, le paysage réglementaire évolue avec l'adoption de normes ouvertes, d'interfaces de programmation d'applications financières (FAPI) et de la confidentialité fondée sur le consentement. Parallèlement, les risques liés à la cybersécurité sont omniprésents.

L'ampleur, la portée et le rythme de ce changement de paradigme, encore accéléré par la pandémie de COVID-19, créent de nouvelles opportunités et de nouveaux risques pour les entreprises du secteur financier. La transformation digitale doit se faire rapidement afin d'améliorer l'expérience client tout en évitant de perturber la stratégie et les opérations de l'entreprise. Les systèmes patrimoniaux autogérés qui posent les plus grands risques de sécurité doivent être éliminés rapidement sans entraver le programme de changement informatique plus large. L'identité numérique doit protéger l'accès aux ressources, applications et données sensibles tout en évitant les frictions inutiles pour les clients. L'écosystème FinServ au sens

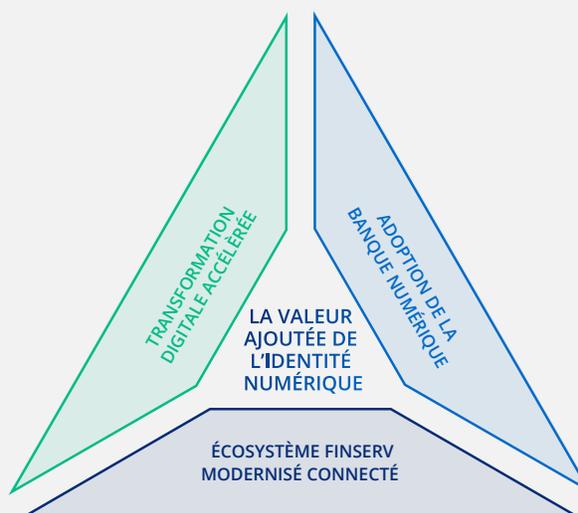
large doit être suffisamment souple pour résister aux changements liés à l'offre et à la demande, tout en étant suffisamment résilient pour atténuer les risques émergents en matière de cybersécurité. Les parcours numériques doivent évoluer en permanence pour alimenter l'acquisition, la conversion et la fidélisation des clients tout en veillant à ce que ces derniers aient le contrôle sur leurs données. L'immobilisme n'est plus une option, car l'ensemble du secteur financier est en train d'être réimaginé.

Explorons ensemble comment ForgeRock accompagne les entreprises à comprendre le potentiel de l'identité numérique pour aider leurs clients, leurs collaborateurs, les tiers de confiance (TTP), leurs partenaires et les identités non humaines à accéder en toute sécurité et en toute simplicité à l'écosystème FinServ connecté. Les fonctionnalités des solutions ForgeRock et l'expérience acquise en matière de création de valeur pour nos clients du secteur financier nous placent dans une position unique pour vous aider à :

- Accélérer la transformation digitale
- Favoriser l'adoption de la banque numérique
- Moderniser l'écosystème des services financiers connectés

« En simplifiant nos anciens systèmes et en les consolidant sur ForgeRock Identity Platform, nous pouvons accélérer la mise en œuvre et l'introduction de nouveaux services, réduire les coûts d'intégration et fournir aux clients des identifiants numériques sécurisés et faciles à utiliser. Nous plaçons l'identité numérique au cœur de nos systèmes. »

Alan Chiew
Directeur Exécutif et Responsable de la Technologie,
Standard Chartered



Libérer le potentiel de l'identité numérique dans les services financiers

ForgeRock permet à tous d'accéder en toute sécurité et en toute simplicité au monde connecté. Nous nous efforçons de remplir cette mission en permettant des expériences numériques exceptionnelles, une sécurité sans compromis et des fonctionnalités complètes à n'importe quelle échelle avec des implémentations simples et flexibles dans des environnements autogérés, tout cloud ou hybrides.

Mais comment l'identité numérique peut-elle contribuer à atténuer les risques et à exploiter les opportunités auxquelles sont confrontées les entreprises des services financiers aujourd'hui ? Pour le comprendre, il faut examiner de plus près les défis auxquels le secteur est confronté.



Optimiser la transformation digitale : Le défi

Le secteur financier se trouve au beau milieu de la transformation la plus disruptive depuis l'avènement des cartes de paiement au début des années 1960. Les changements induits par le marché en Amérique du Nord et les changements induits par la réglementation en Europe et en Asie-Pacifique, ainsi que la disruption stimulée par les startups émergentes des technologies financières (FinTech) ont mobilisé l'innovation technologique. Le marché mondial des FinTech devrait passer de [127,66 milliards de dollars en 2018 à 309,98 milliards de dollars en 2022](#), à un taux de croissance annuel composé (TCAC) de 24,8 %. Là où de nombreuses entreprises financières installées considèrent ces changements comme des menaces existentielles, d'autres y voient une opportunité de proposer des expériences personnalisées et augmenter l'upselling, sans avoir besoin de développer et déployer en interne. Cela permet non seulement d'améliorer l'agilité de l'entreprise et le déploiement continu de nouvelles fonctionnalités, mais aussi de permettre d'exploiter les dernières innovations FinTech.

L'émergence du mouvement Open Banking dans l'Union Européenne (UE), déclenché par le Règlement Général sur la Protection des Données (RGPD) et la Directive révisée sur les Services de Paiement (DSP2) ont poussé le secteur à adopter de nouveaux modèles commerciaux, à réaligner les investissements dans les plateformes bancaires, à adopter des stratégies cloud-natives et, surtout, à intégrer les TTP au cœur de l'écosystème FinServ. Ces capacités donnent aux entreprises les moyens de proposer à leurs clients des offres hyper personnalisées et à valeur ajoutée à un rythme soutenu.

Il n'est pas surprenant de voir que le marché de l'Open Banking devrait être multiplié par six, passant de [7,29 milliards de dollars en 2018 à 43,15 milliards de dollars d'ici à 2026](#).

Pourcentage de banques qui prévoient d'activer et d'exploiter les FAPI ouvertes

	2020	Variation /2019
 US	92%	+23%
 RO	85%	+17%
 Hong Kong	89%	-
 France	87%	-1%
 Allemagne	75%	-4%

[Finastra](#)

Alors que les entreprises FinServ de ces marchés s'alignent sur les exigences réglementaires, elles cherchent à développer leurs capacités, leurs connaissances et leurs écosystèmes afin d'offrir des expériences numériques hyper personnalisées et des offres à valeur ajoutée dans le paysage émergent de l'Open Finance.

Dans d'autres zones géographiques, comme aux États-Unis et au Canada, où la transformation est dictée par les forces du marché et les meilleures pratiques réglementaires - non contraignantes, le secteur financier continue à investir massivement dans les FAPI, les fonctionnalités bancaires mobiles, l'identité fédérée (OpenID Connect et OAuth 2.0) et dans l'infrastructure cloud-native. Ces investissements permettent de proposer des offres personnalisées à valeur ajoutée qui répondent directement aux besoins financiers connus et inconnus de leurs clients et augmentent les taux de conversion, la fidélité et, au final, le chiffre d'affaires. Le début de la pandémie de COVID-19 a encouragé les organisations traditionnelles du secteur financier à déplacer leurs investissements des sites physiques/succursales/agences vers les canaux numériques. Un pourcentage important de ces budgets aux États-Unis est destiné à faire passer les entreprises du secteur financier de l'utilisation du *screen scraping*¹ (capture de données d'écran) à des FAPI sécurisées. Cela permet d'atténuer les risques inhérents, tout en donnant aux clients un plus grand contrôle sur leurs données personnelles et sur leur vie privée, ce qui renforce encore leur fidélité. Dans l'ère post-pandémique, ces fonctionnalités sont de plus en plus exploitées pour protéger la croissance du chiffre d'affaires contre l'augmentation des défaillances de crédit et la persistance des taux d'intérêt bas.

La confluence de ces facteurs a poussé les clients à exiger des expériences simplifiées, sécurisées et personnalisées dans les services bancaires et non bancaires. Dans ce contexte, les clients exigent un renforcement de la confidentialité et de la sécurité, ainsi que la possibilité de contrôler avec qui et quand leurs données sont partagées et dans quel but. Parallèlement, l'évolution vers des canaux de distribution numériques et hybrides, physiques et numériques, a renforcé l'importance de l'engagement omnicanal. En effet, [McKinsey](#) montre que plus de 71 % des clients des banques préfèrent ces canaux aux expériences traditionnelles en agence, et 25 % optent pour un engagement purement numérique. La capacité à offrir des expériences omnicanales exceptionnelles peut faire la différence entre gagner et perdre des parts de marché.

Dans le même temps, l'échelle, la portée et la sophistication des cyberattaques et des fraudes d'identité augmentent. La pandémie de COVID-19 a entraîné une augmentation de [238 %](#) des cyberattaques visant les organisations bancaires rien que de février à avril 2020. Des [données](#) supplémentaires montrent que le secteur des services financiers est 300 fois plus susceptible d'être visé par une cyberattaque que les autres secteurs. Ce risque est encore aggravé par la croissance de l'écosystème FinServ qui crée un potentiel d'attaque tout aussi croissant. La sécurisation des données des clients, de la vie privée et de l'écosystème FinServ est devenue essentielle à l'activité. Les cyberattaques les plus courantes proviennent de la compromission des informations d'authentification et d'un accès non autorisé. En effet, le [rapport ForgeRock 2021 sur les atteintes à l'identité des consommateurs](#) estime que plus de 43 % de toutes les failles dans le monde peuvent être attribuées à un accès non autorisé, le coût moyen s'élevant à 8,64 millions de dollars aux États-Unis et à 3,86 millions de dollars dans le reste du monde. La capacité à exploiter pleinement les forces du marché et de la réglementation qui régissent l'industrie du secteur financier peut contribuer à la flexibilité de l'entreprise, au time-to-market et à la croissance du chiffre d'affaires. Des capacités permettant en retour d'améliorer l'expérience client et de réduire le nombre croissant de cyberattaques. Pour y parvenir, une stratégie et une infrastructure évolutive pour la gestion de l'identité numérique au cœur de l'écosystème est nécessaire.

¹https://en.wikipedia.org/wiki/Data_scraping



Optimiser la transformation digitale : La solution

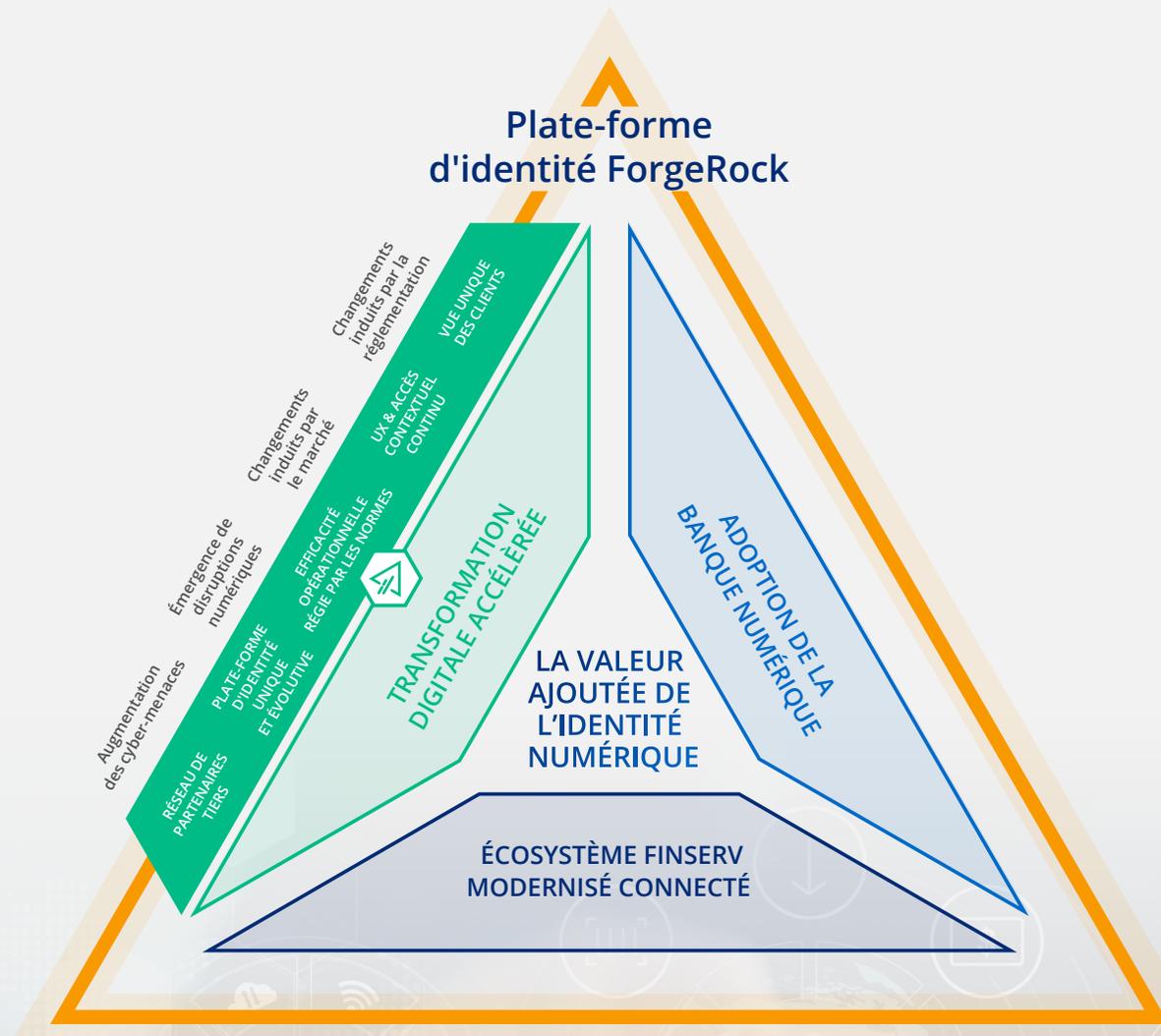
ForgeRock vous accompagne pour relever tous ces défis et accélérer votre transformation digitale grâce à l'identité numérique :

- 1. Fournir une vue unique des clients :** Rassemblez plusieurs sources d'identités pour créer une vue unique des besoins de vos clients, permettant l'hyperpersonnalisation de vos offres à valeur ajoutée tout en rationalisant les parcours et l'expérience client de bout en bout. Unifiez, faites évoluer et sécurisez les annuaires pour assurer des performances et une résilience élevées au sein de services distribués à l'échelle mondiale. Profitez des fonctionnalités de gestion des identités les plus efficaces pour automatiser le cycle de vie complet de milliards d'identités stockées. Exploitez des capacités étendues de synchronisation et de réconciliation des identités pour fournir un écosystème unifié permettant une vision en temps réel des besoins de vos clients. ForgeRock peut faire tout cela grâce à une seule plateforme.
- 2. Améliorer l'expérience des utilisateurs grâce à un accès contextuel et continu aux services :** Offrez aux clients et aux collaborateurs un large choix de méthodes d'authentification, y compris via des identités sociales (réseaux sociaux) et des identités validées par des tiers, pour améliorer simultanément l'expérience utilisateur et la sécurité. Intégrez des signaux contextuels dans les parcours d'authentification avec une interface intuitive d'accès intelligent, sans code et par glisser-déposer, pour personnaliser et sécuriser les expériences de vos utilisateurs.
- 3. Améliorer l'efficacité opérationnelle grâce à des normes ouvertes :** Tirez parti d'une suite complète de fonctionnalités basées sur des normes, notamment OpenID Connect, OAuth 2.0, Security Assertion Markup Language (SAML) et User-Managed Access (UMA) 2.0 pour répondre aux besoins d'authentification, d'autorisation et de réglementation. Offrez à vos clients et à votre personnel une expérience d'authentification unique (SSO), unifiée et fluide pour rationaliser l'accès à plusieurs applications basées sur le cloud. Sécurisez les FAPI avec un chiffrement des données en transit et au repos, une limitation du débit, une authentification configurable et des contrôles d'autorisation.
- 4. Exploiter une plateforme d'identité unique et évolutive pour tous les utilisateurs :** Exploitez les riches fonctionnalités de ForgeRock pour unifier et sécuriser toutes les identités numériques (clients, personnel, partenaires, appareils connectés) dans un environnement cloud et hybride autogéré. Déployez à un rythme maîtrisé et réduisez le délai de mise sur le marché sans être freiné-e par les solutions existantes.
- 5. Sécuriser et accélérer l'intégration tierce :** Bénéficiez de l'innovation collective émanant du réseau de partenaires en identité numérique de ForgeRock et de son écosystème d'intégrations tierces prédéveloppées, testées et dynamiques pour profiter des capacités d'*identity-proofing*, de gestion des risques, de biométrie et d'authentification forte tout en sécurisant et en améliorant les expériences numériques.

« Ce qui est génial avec la solution ForgeRock, c'est que c'est tellement extensible ! Vous pouvez faire à peu près tout ce que vous voulez avec, et si vous n'y parvenez pas, les équipes travailleront avec vous pour que cela se produise. »

Sean Carrick,
VP, Identity Operations
& Engineering, LPL Financial

Accélérer votre transformation digitale avec ForgeRock vous permet de maximiser le retour sur investissement (ROI) des FAPI, de vous aligner sur les réglementations relatives à l'Open Banking et à la protection des consommateurs, et à pleinement exploiter l'innovation FinTech pour maintenir un avantage concurrentiel et atténuer les risques de cybersécurité.





Accélérer l'adoption de la banque numérique : Le défi

L'adoption grandissante des objets connectés intelligents, l'omniprésence de l'accès à distance à Internet et l'émergence du cloud ont alimenté la croissance exponentielle des challengers de la banque numérique dans toute la zone Asie-Pacifique, en Amérique Latine, en Europe et dans une moindre mesure, en Amérique du Nord. Une [étude](#) a prévu que le secteur des banques challengers et des néobanques passera de 20,4 milliards de dollars en 2019 à 471 milliards de dollars d'ici à 2027, à un taux de croissance annuel composé (CAGR) de 48,1 %. Toutefois, la croissance soutenue dépend en grande partie de la capacité de ces banques à acquérir et à convertir plus de [1,7 milliard de consommateurs non bancarisés](#) dans le monde, ainsi qu'à étendre leur portée aux consommateurs sous-bancarisés. En Indonésie, par exemple, plus de 81 % des gens possèdent un appareil mobile, mais seulement [48,9 % ont un compte bancaire](#). Aux États-Unis, les consommateurs sous-bancarisés représentent [plus de 16 %](#) de la population. Et [62 %](#) de la population européenne envisage de passer de la banque physique à la banque numérique. Garder une longueur d'avance sur la concurrence peut faire la différence entre le maintien des fonds d'investissement pour l'expansion et la perte de pertinence.

Parallèlement, l'essor de la banque numérique a stimulé la croissance des néobanques, soutenues par des fournisseurs de services bancaires établis et des start-ups FinTech qui cherchent à conquérir des parts de marché. Ces organisations s'appuient sur les meilleures technologies cloud-natives, sur l'hyperpersonnalisation et sur des stratégies marketing innovantes pour offrir aux clients des expériences fluides qui trouvent un écho auprès des Millenials, de la génération Z et, de plus en plus, auprès de la génération X et des baby-boomers. En éliminant les frictions dans les expériences des utilisateurs, les banques peuvent déployer des expériences centrées sur le numérique et sur le mobile à [75 % du coût](#) supporté par la banque de détail traditionnelle. Malgré la demande croissante de services bancaires numériques, le secteur continue de se heurter à des obstacles systémiques encore amplifiés par la pandémie. En effet, les banques challengers ont du mal à monétiser et à développer des services à valeur ajoutée en s'éloignant des modèles de revenus basés sur les transactions.

Les jeunes banques FinTech réglementées, quant à elles, continuent de financer leur expansion par le biais du capital-risque, tandis que les banques traditionnelles retiennent leurs investissements car le marché se consolide inévitablement. Pour gagner des parts sur les marchés du non-bancarisé et du sous-bancarisés, les banques traditionnelles créent plutôt des banques de type « challenger » et se lancent dans la banque numérique. Cette tendance, amplifiée par la pandémie, a obligé les banques

53%



de la population mondiale utilisent plus les applications bancaires qu'avant la pandémie.

[Mastercard](#)

à continuellement améliorer les expériences digitales et les offres à valeur ajoutée qu'ils proposent à leurs clients. Pour conserver un avantage concurrentiel, il est essentiel de conquérir des parts de marché et de diversifier les sources de revenus grâce à des expériences sécurisées, transparentes et hyper-personnalisées.

Les business modèles mis à part, le défi le plus important auquel sont confrontées les banques numériques est peut-être de pouvoir conserver la confiance des clients. [Quarante-cinq pour cent](#) des consommateurs pensent que les banques challengers cesseront d'exister à court terme, et seuls 10 % d'entre eux leur font confiance pour gérer leurs données en toute sécurité, contre 41 % pour les banques traditionnelles. Les banques challengers s'appuient sur des accords opaques d'e-connaissance du client (eKYC) et sur des intégrations d'écosystèmes avec des TTP pour prouver l'identité de leurs nouveaux clients, et leurs règles d'authentification et d'autorisation faibles créent des risques de cybersécurité et de fraude d'identité qui menacent de compromettre la confiance des clients. Le [ForgeRock Consumer 2021 Identity Breach Report](#) montre que les attaques impliquant des noms d'utilisateur et des mots de passe ont augmenté de 450 % d'une année sur l'autre – y compris pour les banques challengers numériques - le secteur le plus ciblé, juste derrière le secteur de la santé.

Pour devancer la concurrence dans un secteur bancaire numérique en pleine mutation, il faut être capable d'améliorer l'expérience client de bout en bout en proposant et en convertissant à un rythme soutenu des offres personnalisées à valeur ajoutée en fonction des besoins des consommateurs. Pour y parvenir, il faudra disposer d'une stratégie et d'une infrastructure pour l'identité numérique complètes et évolutives au cœur de l'écosystème.



Accélérer l'adoption de la banque numérique : La solution

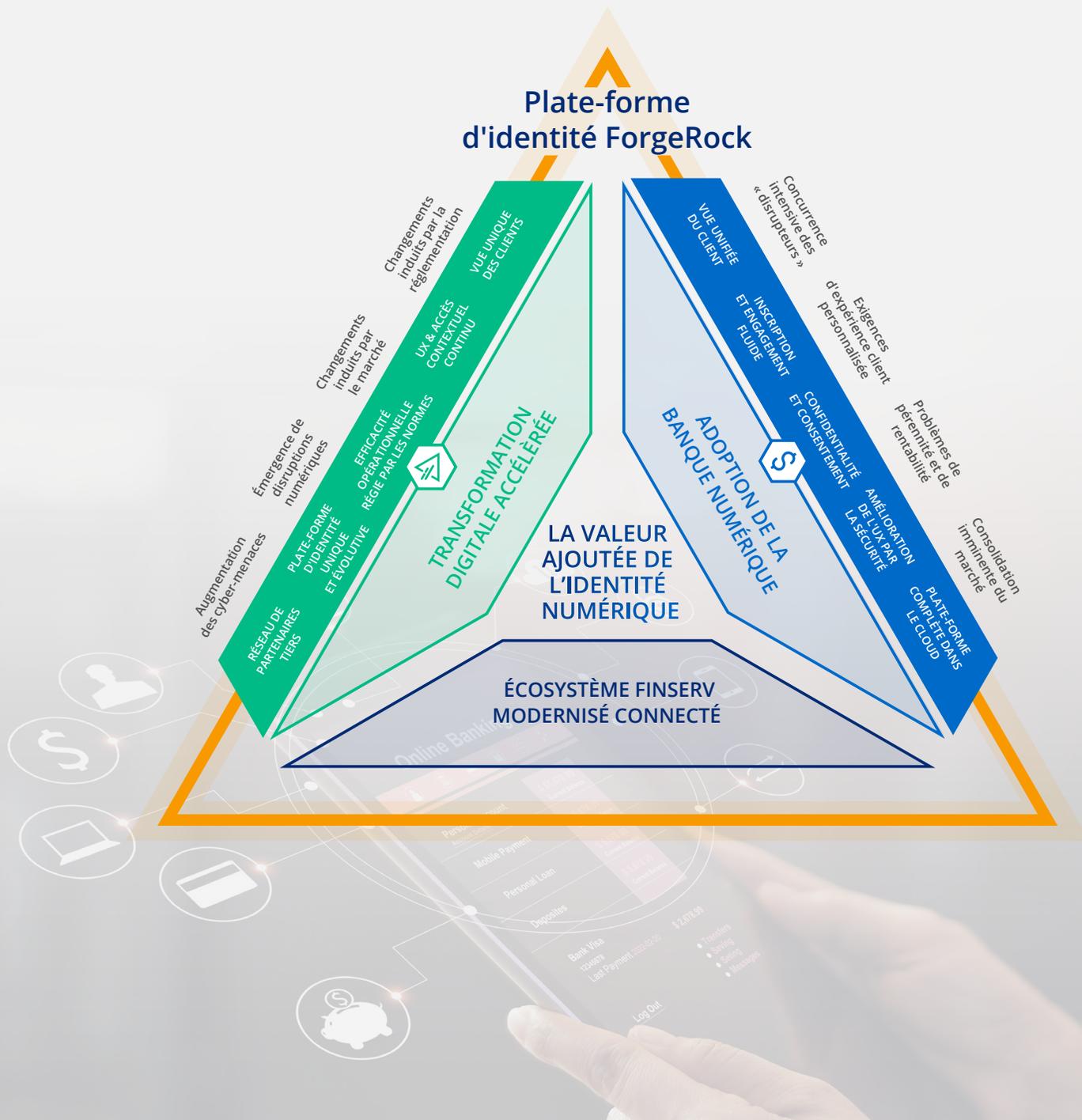
ForgeRock vous accompagne pour relever tous ces défis et accélérer votre transformation digitale grâce à l'identité numérique :

- 1. Fournir une vue unique des clients sur tous les canaux :** Créez une vue unifiée des besoins, des comportements et des préférences de vos clients. Hyper-personnalisez des offres intégrées à valeur ajoutée afin de stimuler la vente incitative auprès des clients existants et d'attirer rapidement de nouveaux clients. Les parcours utilisateurs peuvent être configurés de manière centralisée et mis à disposition sur tous les canaux avec facilité et cohérence, que les clients utilisent un smartphone, un ordinateur portable, un kiosque, un système vocal ou tout autre appareil connecté.
- 2. Faciliter l'inscription et l'engagement des utilisateurs :** Augmentez les taux de conversion en facilitant l'inscription grâce à des options d'inscription via les réseaux sociaux. Supprimez les formulaires trop longs et appliquez un profilage progressif après la connexion, permettant aux clients de fournir des informations riches au fil du temps. Proposez plusieurs options d'authentification afin que les clients puissent interagir avec les services et les centres d'appels plus rapidement. Proposez des fonctions de libre-service faciles à utiliser, notamment des options de mot de passe, de sécurité, de marketing, de profil et de confidentialité.
- 3. Renforcer la confidentialité et le consentement :** Donner aux clients le contrôle sur leurs données - de l'accès à leurs comptes jusqu'à la gestion des paramètres de profil et de confidentialité - est essentiel pour la plupart des solutions orientées client. La gestion de la confidentialité et du consentement permet d'établir une relation plus étroite avec les clients car ils peuvent voir quelles informations personnelles une entreprise détient et pourquoi. Cela permet en parallèle de réduire les coûts liés au support clients. ForgeRock fournit un tableau de bord complet de gestion des profils et de la confidentialité, basé sur les normes et législations locales. Les utilisateurs peuvent gérer qui a accès à leurs données personnelles, pour combien de temps et dans quelles circonstances. Ils peuvent également gérer les détails de leur propre profil, les appareils connectés à leur compte, et les applications qu'ils ont consenties à connecter à leur compte.
- 4. Améliorer l'expérience grâce à la sécurité :** Offrez des expériences client transparentes, sécurisées et personnalisées en permettant un parcours fluide grâce à l'authentification sans nom d'utilisateur, ni mot de passe, multifactorielle et reposant sur l'appareil utilisé. Exploitez les signaux contextuels, tels que la localisation, l'adresse IP, le type d'appareil, le système d'exploitation et le type de navigateur pour déclencher une authentification adaptative, protégeant ainsi vos clients tout en éliminant les frictions inutiles sur leur parcours. Sécurisez les transactions de grande valeur grâce à une authentification forte basée sur le contexte et à des workflows d'autorisation push mobiles pour renforcer la confiance et la sécurité. Assurez-vous que les données personnelles de vos clients sont sécurisées, tant au repos qu'en transit dans votre écosystème, afin d'atténuer le risque de violation et d'usurpation d'identité.
- 5. Exploiter les fonctionnalités complètes de ForgeRock Identity Platform dans le cloud :** Veillez à ce que vos clients puissent bénéficier d'un déploiement continu et rapide de nouvelles fonctionnalités et offres en tirant parti de la boîte à outils de développement logiciel (SDK) mobile de ForgeRock pour intégrer les puissantes fonctionnalités de la plateforme dans les applications orientées client. Sécurisez les données de vos clients avec une passerelle de sécurité FAPI dans votre environnement hybride pour garantir la confiance et la fidélité des clients tout en respectant les exigences réglementaires. Améliorez les performances de vos applications clients grâce à ForgeRock Identity Cloud, et répondez aux pics d'activité grâce à une architecture cloud multi-tenants, mais avec une isolation totale des données de chaque client. Bénéficiez de la plateforme de gestion des identités et des accès la plus performante pour gérer, unifier et sécuriser toutes les identités numériques dans un environnement hybride, afin de minimiser la charge liée à l'existant et d'accélérer le time to value.

« La sécurité est essentielle pour intégrer rapidement de nouveaux clients et de nouvelles entreprises, de même que pour offrir une expérience numérique idéale. Avec sa solution de gestion des identités et des accès clients (CIAM) pour nos applications Jenius, ForgeRock nous aide à développer notre activité au-delà de nos attentes. »

Joko Kurniawan, Senior Vice Président, IT Digital Service Enablement, BTPN Bank

Le pilotage de la banque digitale avec ForgeRock vous permet de maximiser vos investissements numériques, d'hyper-personnaliser les offres à valeur ajoutée et d'exploiter pleinement l'innovation FinTech pour générer de nouveaux revenus, accroître votre part de marché et atténuer le risque lié aux cyber-menaces.





Moderniser l'écosystème des services financiers connectés : Le défi

À mesure que le rythme de la transformation digitale s'accélère et que sa portée s'étend, votre écosystème deviendra inévitablement plus coûteux et plus difficile à gérer, ce qui accroîtra votre vulnérabilité face aux menaces émergentes.

La gestion d'une liste toujours plus longue d'identités de salariés, de TTP (tiers de confiance), de partenaires et de demandes d'accès au cœur et à la périphérie de l'écosystème FinServ peut submerger les équipes informatiques et entraîner une [dérive du respect strict des droits](#). Cela peut exposer les organisations à des risques excessifs lors de l'extension des infrastructures numériques, des fonctionnalités et des offres à valeur ajoutée. Les études montrent que les écosystèmes numériques [les plus performants](#) sont composés en moyenne de 40 partenaires et TTP, dont 77 % couvrent les marchés émergents et 83 % s'étendent sur plusieurs secteurs d'activité. La sécurisation et l'automatisation du cycle de vie de la gestion des accès de bout en bout avec les dernières technologies utilisant l'intelligence artificielle (IA) contribuent à améliorer l'agilité de l'entreprise, à réduire les coûts et à garantir la conformité aux exigences réglementaires, telles que le Règlement Général sur la Protection des Données (RGPD) en Europe et la loi Sarbanes-Oxley, entre autres.

La gestion des droits, la mise en place d'une séparation des tâches (SOD) et la prévention des accès non autorisés deviennent de plus en plus coûteuses et difficiles à gérer. Le rapport [2021 Varonis Data Risk report](#) pour les services financiers montre que chaque employé du secteur a, en moyenne, accès à plus de 11 millions de fichiers. De plus, 63 % des entreprises du secteur financier laissent plus de 1 000 fichiers sensibles accessibles à chaque employé, sans gestion des accès, ni gouvernance des identités de base pour minimiser le risque que cela représente. Par ailleurs, les [recherches](#) montrent que 65 % des comptes internes compromis n'ont pas été consultés depuis plus de 90 jours, ce qui suggère qu'ils sont, soit inactifs, soit qu'ils doivent être dé-provisionnés de manière urgente. La centralisation, l'automatisation et l'élimination des risques d'accès dans l'écosystème FinServ sont plus importantes que jamais. Les progrès de l'IA, de l'apprentissage automatique (ML) et l'adoption progressive des technologies cloud sont des facteurs déterminants qui ont poussé les organisations FinServ à augmenter leurs investissements dans la gouvernance et l'administration des identités (IGA) ainsi que dans les fonctionnalités de gestion des accès internes (AM). Cela leur permet de gérer efficacement le cycle de vie des identités de bout en bout, de mobiliser un large éventail de politiques SOD, de contrôles de sécurité et de réduire le laisser-aller dans le respect des droits afin d'améliorer

43%



**de toutes les violations de données
sont attribuées à un accès non
autorisé.**

[2021 ForgeRock Consumer Identity
Breach Report](#)

leur agilité, de réduire les coûts et de rester en conformité réglementaire.

Malheureusement, une technologie vieillissante de gestion des identités et des accès (IAM) présente des obstacles et entraîne des retards. La perspective de désinstaller et de remplacer les anciens systèmes IAM est décourageante. L'abandon des systèmes existants de gestion des identités et des accès est intrinsèquement risqué pour toute organisation. Pour atténuer ces risques, les organisations FinServ doivent trouver des moyens efficaces et rapides de protéger leurs clients contre des perturbations inutiles, en isolant leur entreprise des dépassements de coûts et des problèmes potentiels d'audit de conformité interne. ForgeRock accompagne ces organisations à accélérer cette migration des identités par un facteur de plus de 30 % grâce aux accélérateurs ForgeRock *Modernize IAM*. Ces accélérateurs peuvent aider les entreprises à éviter une expérience douloureuse de remplacement et leur permettre d'orchestrer une migration planifiée et ciblée vers la plateforme ForgeRock afin d'éviter les interruptions de service, de réduire les coûts et d'accélérer la création de valeur. Plus important encore, ils peuvent accélérer aussi le retour sur investissement de la modernisation digitale et permettre aux clients de bénéficier de nouvelles fonctionnalités et offres en quelques jours plutôt qu'en plusieurs mois voire années.

L'immobilisme n'est plus une option, car votre écosystème évolue pour faire face à la concurrence. En adoptant l'« [identity fabric](#) » en pleine expansion, vous pouvez mettre en place un ensemble complet de fonctionnalités pour la gestion de l'identité numérique afin d'accélérer l'accès sécurisé du personnel, des TTP et des partenaires, afin de se conformer aux réglementations, d'atténuer les risques et de réduire les coûts.

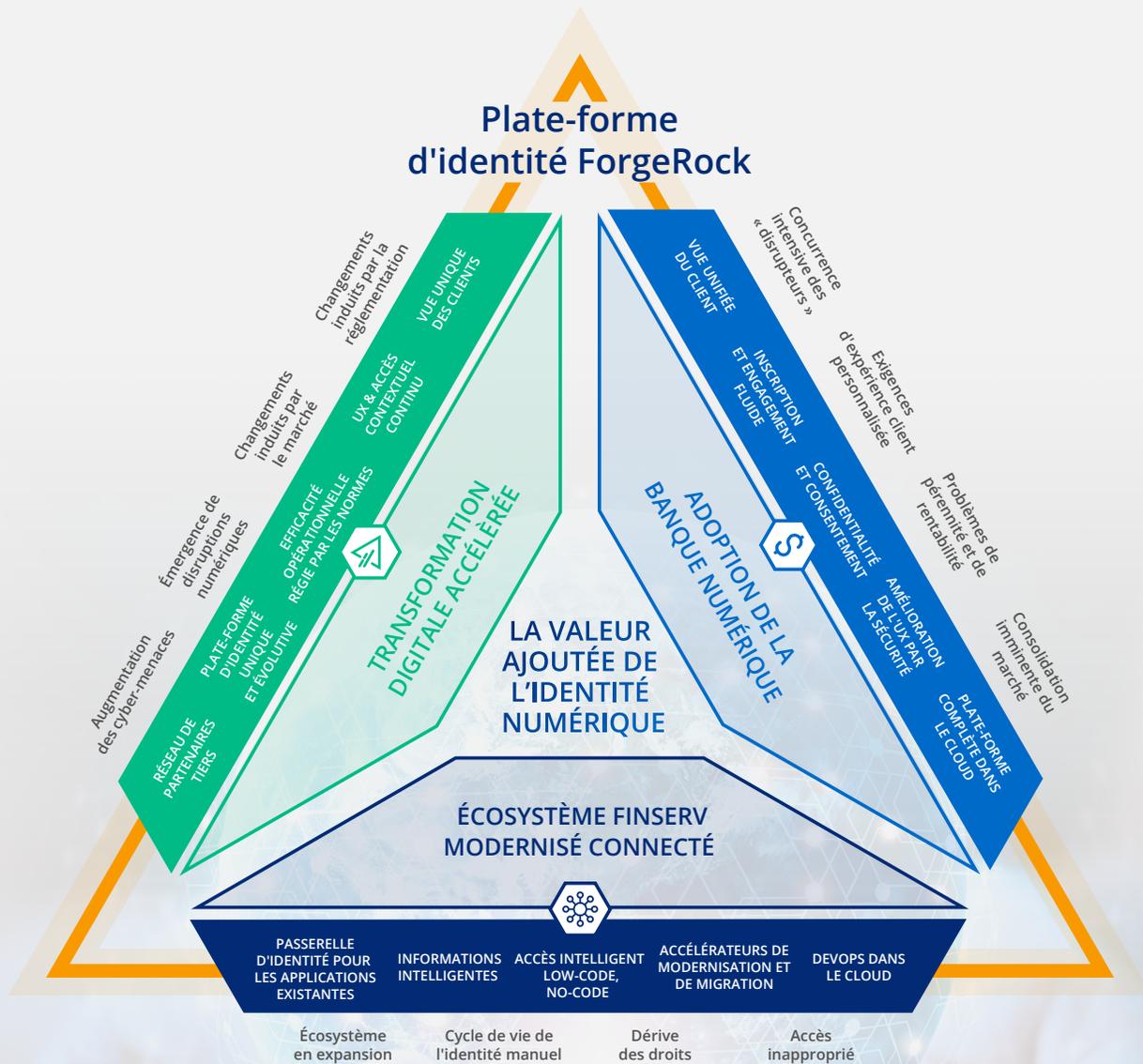


Moderniser l'écosystème des services financiers connectés : La solution

ForgeRock vous accompagne pour relever tous ces défis et accélérer la modernisation de votre écosystème de services financiers grâce à l'identité numérique :

- 1. Tirer parti de l'intelligence artificielle :** Utilisez la gouvernance des identités pilotée par l'IA pour l'ensemble du personnel, des tiers de confiance et des partenaires et restez en conformité réglementaire, atténuez les risques et réduisez les coûts. Automatisez les validations d'accès à haut niveau de confiance, recommandez la certification pour les comptes à faible risque et automatisez la suppression des rôles inutiles afin de sécuriser et d'optimiser la gouvernance des identités numériques, d'éliminer le risque de dérive des droits et de minimiser la validation automatique des certifications d'accès. Exploitez les investissements et les systèmes existants de gouvernance et d'administration des identités (IGA) et augmentez leur efficacité grâce à un moteur intelligent pour automatiser la gestion du cycle de vie complet des identités numériques.
- 2. Accélérer les efforts de modernisation et de migration :** Minimisez l'impact et le risque de la modernisation de vos systèmes en échelonnant la migration complexe de votre IAM existant à l'aide de kits d'outils d'accélération *Modernize IAM* en open-source. Utilisez une gamme complète d'options pour prendre en charge les migrations d'utilisateurs, en masse ou ponctuelle, avec des modèles préconfigurés disponibles sans frais supplémentaires. Orchestrez la migration des identités depuis plusieurs systèmes de gestion des identités vers la plateforme ForgeRock, ce qui permet de bénéficier des investissements existants et de rationaliser les opérations sans aucune perturbation pour les clients. Facilitez l'ouverture rapide et sécurisée des interfaces de programmation d'applications (API) pour l'Open Banking et l'expansion de l'écosystème pour les workflows d'inscription, de consentement et d'autorisation d'accès afin de tirer pleinement parti des investissements et de l'agilité des FAPI.
- 3. Intégration et sécurisation des applications existantes :** Simplifiez et sécurisez la manière dont votre personnel, les TTP et les partenaires s'authentifient et accèdent aux applications existantes en activant des fonctionnalités complètes de SSO et de fédération pour accélérer la transformation digitale, réduire le time-to-value et sécuriser les API. Exploitez les puissantes fonctionnalités de la passerelle d'identité pour protéger vos services et applications contre les attaques par déni de service distribué (DDoS), contrôlez le trafic des API, limitez la demande et détectez les anomalies de manière proactive.
- 4. Permettre un accès intelligent low-Code, no-Code :** Utilisez un puissant concepteur visuel doté d'une interface glisser-déposer pour configurer, orchestrer et sécuriser facilement les parcours des employés, des TTP et des partenaires en utilisant rapidement un large éventail d'authentificateurs prêts à l'emploi. Cela élimine le besoin de codage et réduit considérablement le temps de valorisation. Exploitez un vaste écosystème d'intégrations tierces pour renforcer les fonctionnalités d'authentification forte, de biométrie comportementale, de gestion des risques et de vérification de l'identité. Intégrez des signaux contextuels, tels que la localisation, l'adresse IP, le type d'appareil, le système d'exploitation et le type de navigateur, dans les parcours d'authentification pour améliorer l'expérience et la sécurité. Tirez parti des signaux contextuels pilotés par l'IA, de la connaissance des accès des utilisateurs à haut risque et des recommandations de remédiation pour introduire des niveaux appropriés de friction d'accès et protéger l'écosystème FinServ contre les accès non autorisés.
- 5. Mise en œuvre d'un modèle cloud de DevOps :** Exploitez la puissance de Docker et Kubernetes en utilisant les options de déploiement IAM multi-cloud les plus rapides et les plus flexibles pour accélérer le délai de mise sur le marché, déployer des millions d'identités en quelques minutes sur n'importe quel cloud et réduire considérablement les coûts de mise en œuvre. Prenez en charge tous les types d'identité dans n'importe quel cloud, et permettez le développement rapide et reproductible de solutions pour soutenir les déploiements DevOps. Cela permet une évolutivité, une flexibilité accrue et, au final, aide à apporter de la valeur aux clients plus rapidement et à moindre coût.

La modernisation de votre écosystème de services financiers connectés avec ForgeRock vous aidera à améliorer l'accès sécurisé de votre personnel, des TTP et de vos partenaires afin de respecter la réglementation, d'atténuer les risques et de réduire les coûts.



Conclusion

La confluence des forces du marché et de la réglementation, ainsi que l'émergence de modèles centrés sur le client, d'écosystèmes et de disruption numérique dans le secteur FinServ, signifient que l'agilité de l'entreprise n'est plus un luxe pour maintenir un avantage concurrentiel. Ancrer une stratégie globale de gestion de l'identité numérique au cœur de vos investissements vous permettra d'accélérer la transformation digitale, de favoriser l'adoption de la banque numérique et de moderniser votre écosystème FinServ connecté.

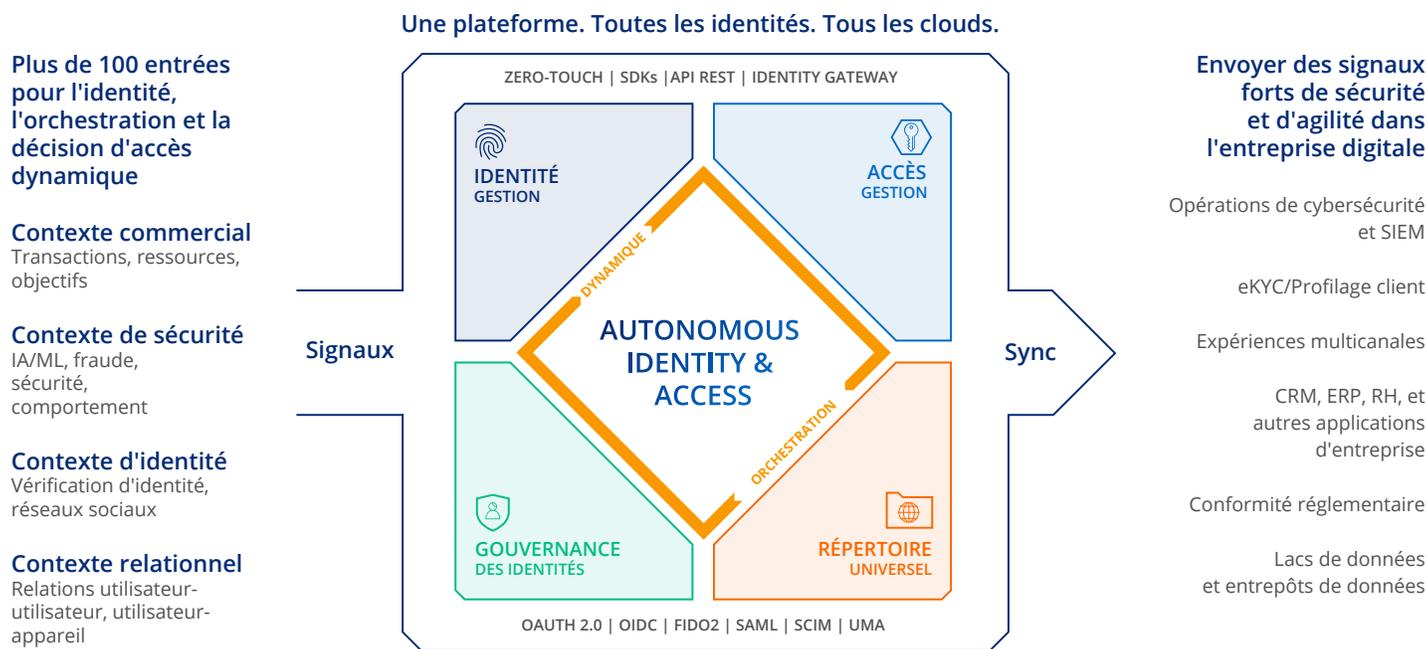
ForgeRock accompagne les organisations pour libérer tout le potentiel de l'identité numérique pour aider les clients, les collaborateurs, les tiers de confiance et les partenaires à accéder en toute sécurité et en toute simplicité à l'écosystème FinServ connecté. Grâce à [ForgeRock Identity Platform](#) leader sur le marché, et de [ForgeRock Hybrid IAM](#) vous pouvez accélérer la transformation digitale,

stimuler la croissance du chiffre d'affaires, offrir des expériences omnicanales exceptionnelles, sécuriser votre écosystème de services financiers et répondre aux exigences réglementaires.

ForgeRock est reconnu comme un leader dans le domaine de la gestion des identités et des accès des clients (CIAM) par [Forrester Wave](#) 2020, le [KuppingerCole](#) Leadership Compass 2020 for CIAM, le Magic Quadrant 2020 de [Gartner](#) pour la gestion des accès, et est un leader global dans le [KuppingerCole](#) Leadership Compass 2021 for Identity Fabric. ForgeRock est idéalement positionné pour accompagner les services financiers à optimiser leur retour sur investissement dans la transformation digitale.

Prenez de l'avance sur vos concurrents en exploitant l'identité numérique au maximum de son potentiel avec ForgeRock.

ForgeRock Identity Platform utilise l'Intelligence Artificielle (IA)



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 et suivez-nous sur les réseaux sociaux.

Suivez-nous !

