

GUIDE EXÉCUTIF

# Cloud de connectivité pour le secteur bancaire :

un nouveau modèle de connexion, de protection et d'accélération des banques



- 3 Tendances et défis du secteur bancaire d'aujourd'hui
- 5 Une nouvelle approche de la résolution des difficultés liées à la sécurité, au développement et à l'informatique moderne
- 6 Améliorez l'agilité de votre entreprise
- 7 Les principaux composants du cloud de connectivité
- 8 Le cloud de connectivité Cloudflare
- 9 Étude de cas : Investec
- 10 Pourquoi choisir Cloudflare ?
- 11 Notes de fin

# Tendances et défis du secteur bancaire d'aujourd'hui

Le secteur bancaire connaît une transformation comme jamais auparavant. La volonté de contribuer au développement durable et l'émergence des nouvelles technologies (p. ex. l'IA, la numérisation et l'informatique cloud) modifient le panorama des services bancaires mobiles, désormais devenus un élément central de l'expérience client.

Pour rester compétitive au sein d'un marché lui aussi affecté par les incertitudes géopolitiques et les mutations de la société, comme la transition vers le travail hybride, votre banque doit innover et rester agile. Cruciale pour s'adapter aux nouvelles conditions, la mise en œuvre de cette approche doit néanmoins s'effectuer sans augmenter les risques.

De même, votre entreprise doit parvenir à réduire la complexité en réunissant ses collaborateurs, ses appareils, ses clouds, ses systèmes, ses applications et ses réseaux distribués. Enfin, il est essentiel pour vous de réaliser la valeur de vos investissements dans la technologie.

La réponse réside dans la mise en place d'un écosystème bancaire unique et unifié, plus simple, plus rapide, plus flexible et plus sûr.

# Tendances et défis du secteur bancaire d'aujourd'hui



## Coûts plus élevés

**1,7M USD** Les entreprises [perdent](#) en moyenne 1,7 million de dollars par an au niveau de leur productivité, car les équipes informatiques et l'entreprise doivent se réunir souvent (12,5 h par semaine) pour rechercher les causes et les solutions à leurs problèmes.<sup>1</sup>

**74 %** des DSI [se disent](#) « fatigués » de devoir compiler les données de multiples outils pour évaluer l'incidence des investissements en matière d'infrastructure informatique.<sup>2</sup>

**75 %** des DSI reconnaissent que leur incapacité à identifier « les dépenses inutiles en matière de SaaS » constitue une menace pour la réussite de leur entreprise.<sup>3</sup>



## Risques accrus

**53 %** des dirigeants du secteur bancaire considèrent les cyberattaques comme le plus grand risque pour leur entreprise.<sup>4</sup>

**99 %** Les analystes [prédisent](#) que d'ici 2025, 99 % des violations au niveau du cloud seront imputées à des erreurs de configuration ou à des erreurs de l'utilisateur final.<sup>5</sup>

**89 %** des RSSI/CSO [déclarent](#) que le déploiement rapide des services numériques a généré des risques imprévus en matière de sécurisation des données.<sup>6</sup>



## Moins de visibilité

**40 %** des entreprises conviennent ou conviennent tout à fait qu'elles perdent le contrôle de leurs environnements informatiques et de sécurité.<sup>7</sup>

**36 %** des DSI et des décideurs en matière d'informatique considèrent que l'intégration des données et des applications cloisonnées représente leur plus grand défi en termes de transformation numérique.<sup>5</sup>

**22 %** des dirigeants du secteur bancaire considèrent que leur entreprise prend du retard dans la réalisation de ses initiatives et de ses objectifs de transformation numérique.<sup>4</sup>

# Une nouvelle approche de la résolution des difficultés liées à la sécurité, au développement et à l'informatique moderne

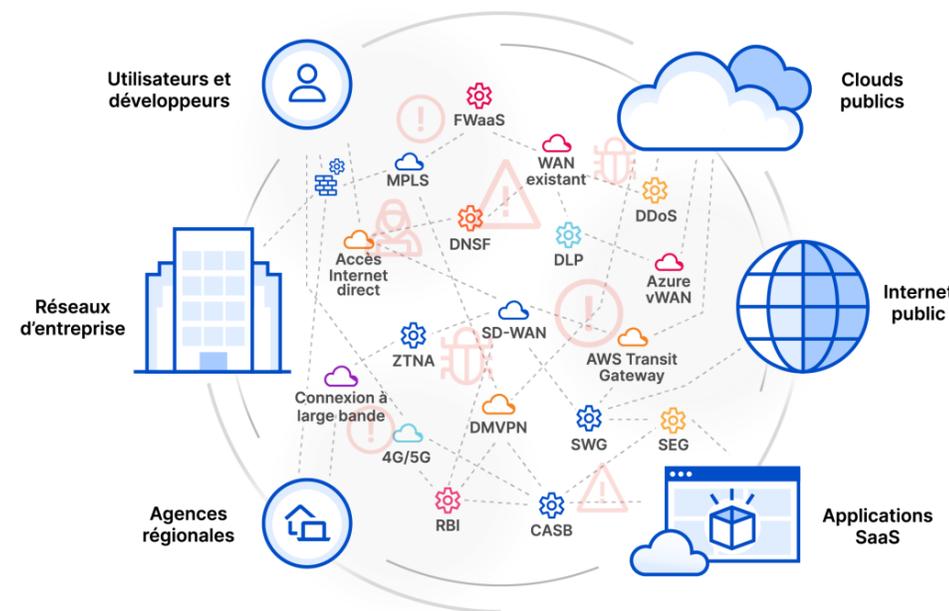
Jusqu'à présent, les banques ont essayé de répondre aux exigences du monde hyperconnecté en mettant en œuvre une combinaison complexe de clouds multiples, de produits dédiés, d'équipements physiques sur site et de fournisseurs de toutes les formes et de toutes les tailles.

Pour reprendre le contrôle, les responsables chargés de l'informatique et de la sécurité ont besoin d'un **nouveau modèle de cloud**. Un modèle qui ne se présente pas à nouveau comme un autre outil complexe à intégrer. Un modèle qui leur offre une **visibilité unifiée** et le contrôle sur chaque domaine dont ils ont la responsabilité.

**Découvrez le cloud de connectivité.**

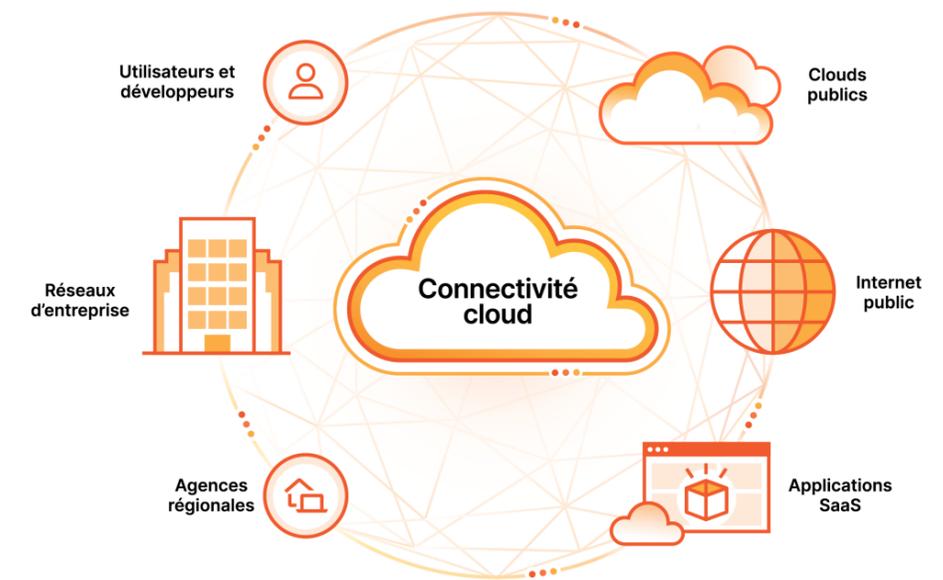
AVANT

Le cloud de connectivité transforme les environnements informatiques fragmentés, présentant un haut niveau de risque, mais un faible degré de contrôle, comme celui-ci :



APRÈS

en un environnement qui garantit le contrôle constant, en proposant un nouveau moyen de connecter, de protéger et d'accélérer de l'entreprise :



## La situation actuelle :

---

Les équipes informatiques et de sécurité sont désormais chargées d'assurer le maintien de la productivité et de la conformité, tout en gérant un environnement de plus en plus complexe. Faute de solutions adéquates, ces difficultés peuvent peser directement sur l'expérience client, la productivité et la compétitivité d'une banque.

---

La complexité des solutions informatiques cloisonnées expose les banques à de **nouvelles menaces internes et externes pour leurs données, leurs applications, leurs réseaux et leur infrastructure**. Les difficultés entourant la régionalisation et la conformité des données augmentent également.

---

La victoire revient cependant toujours aux plus rapides. De nombreuses banques doivent composer avec une dette technique, des contraintes alambiquées au niveau de leur infrastructure, ainsi que des systèmes opaques et complexes qui **entravent l'utilisation et la prestation de services numériques**.



## Connecter



## Avec une connectivité cloud :

---

Le cloud de connectivité permet de **sécuriser et de connecter l'ensemble des ressources d'une entreprise sur une plateforme unique, sans perdre de temps en intégrations complexes ni en solutions de contournement**.

Simplifiez les opérations tout en connectant votre environnement actuel et à venir (collaborateurs, clients, appareils ou systèmes, supports informatiques ou de stockage, technologie traditionnelle ou moderne), de bout en bout.

---

## Protéger



Le cloud de connectivité fournit les fonctions de sécurité, de confidentialité, de conformité et de développement (de même que les informations transversales) nécessaires pour **garder une longueur d'avance sur l'évolution des menaces et des réglementations**.

Elle offre par ailleurs une plus grande visibilité dans tous les secteurs, vous pouvez ainsi **évaluer, contrôler et atténuer le risque avec plus de précision depuis une interface de contrôle unique**.

---

## Accélération



Modifiez radicalement la manière dont les personnes, les technologies et les réseaux se connectent sur l'ensemble des domaines. Le cloud de connectivité **facilite et accélère le travail des équipes qui conçoivent, développent et proposent des applications innovantes, partout dans le monde**.

# Les principaux composants du cloud de connectivité

Les composants architecturaux du cloud de connectivité servent et connectent les collaborateurs, les développeurs, les clients, les partenaires, les environnements multcloud et tous les types de réseau :

## Architecture composable et programmable

- Interopérabilité illimitée
- Réseaux personnalisables

## Intégration à l'ensemble des réseaux, des entreprises et d'Internet

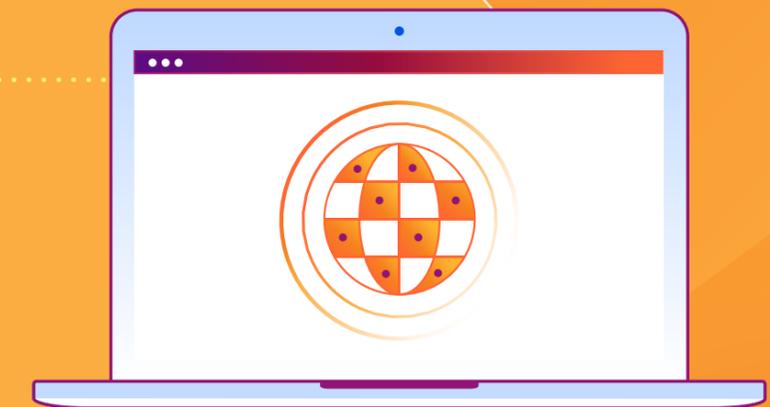
- Contrôle total d'une requête de la source à la destination
- Connectivité réseau évolutive à l'infini
- Services toujours disponibles depuis chaque serveur

## Plateforme intelligente

- Sécurité, performances, confidentialité et conformité intégrées
- Informations transversales sur les menaces et le réseau

## Interface unifiée et simplifiée

- Interface de gestion unifiée sur l'ensemble d'une plateforme produit intégrée
- Journalisation consolidée
- Communication facilitée entre les différentes architectures pendant la migration vers des réseaux totalement Internet-native





## Le cloud de connectivité Cloudflare



Architecture composable et programmable



Intégration à tous les réseaux



Plateforme alliant intelligence et innovations



Interface simple et unifiée



Accès simple et sécurisé



Applications et infrastructure de confiance



Services agiles pour développeurs

- Proxy interne (inline)
- Mesures de contrôle des applications et des API
- Services Edge pour développeurs
- Intégration CDN-WAN-réseau
- Multicloud (SaaS/ IaaS)
- Conformité et confidentialité
- Analyse des données liées au risque
- Protection des données
- Défense contre les menaces

## Réseau mondial programmable de Cloudflare



Intelligence artificielle/ apprentissage automatique



Informations sur les menaces et les réseaux

Services et support mondiaux



# Développer une plateforme de banque ouverte internationale et intégrée



Institution de premier plan dans le domaine des services financiers mondiaux, Investec propose des services internationaux en matière de banque, d'investissement et de gestion de patrimoine à des clients privés, institutionnels et issus du monde de l'entreprise. Ses deux principaux marchés sont l'Afrique du Sud et le Royaume-Uni.

Connue pour son service client exceptionnel, qui lui permet d'offrir une expérience « hautement technologique et personnalisée », Investec place nettement l'accent sur l'innovation technologique. L'entreprise s'est associée à Cloudflare pour développer une nouvelle solution dans le cadre de son engagement en faveur de services bancaires ouverts.



## La difficulté

### Renforcer l'architecture grâce à la migration des solutions vers la périphérie du réseau, de manière sécurisée

Dans le cadre de son expansion stratégique vers les canaux bancaires numériques, la principale préoccupation d'Investec résidait dans le fait de sécuriser et de connecter ses services en ligne à sa base d'utilisateurs internationale. Elle devait assurer la tranquillité d'esprit de ses clients, tout en cherchant des moyens efficaces de développer sa stratégie numérique.



## La solution

### Atténuer les menaces cybercriminelles sophistiquées afin de protéger les données financières de ses utilisateurs

Maintenant que la plateforme Cloudflare Zero Trust connecte et sécurise ses utilisateurs et ses données, Investec peut anticiper et contrer les attaques, mais aussi détourner les tentatives d'implantation de rançongiciels, le phishing, les exploitations de vulnérabilités zero-day et bien davantage. Les outils de sécurité de la couche 7 proposés par Cloudflare sécurisent encore davantage le site web et l'application d'Investec, afin d'améliorer la visibilité et la protection de l'infrastructure informatique.



## Principaux résultats

- Sécurisation des données bancaires et financières des utilisateurs contre les attaques en ligne.
- Amélioration de l'expérience client en soutenant le développement des premiers outils programmables par l'utilisateur du secteur.
- Réduction des efforts de développement et du délai de mise sur le marché des innovations concernant les produits.
- Simplification du développement stratégique à long terme et de la planification de la sécurité.

► [Consultez l'étude de cas dans son intégralité ici.](#)

# Choisissez Cloudflare pour connecter, protéger et accélérer votre banque

« Nous avons rapidement remarqué que nous pouvions réduire notre complexité opérationnelle avec Cloudflare. En faisant migrer toutes nos ressources vers le cloud de connectivité Cloudflare, nous avons rationalisé la gestion des services et amélioré notre sécurité, tout en limitant le risque d'erreur humaine. »

**Kristian Petersen**  
SRE Team Lead, EQT

« La solution Cloudflare Access nous permet de bénéficier d'un processus d'authentification Zero Trust, de mesures de contrôle des accès granulaires et d'une visibilité complète sur l'activité de nos utilisateurs. Elle est essentielle à la mise en place du Zero Trust, qui reconnaît que les menaces peuvent être aussi bien internes qu'externes. »

**Christian Trummer**  
CTO et cofondateur, Bitpanda

« La plateforme Cloudflare est conçue par des développeurs, pour des développeurs. Ce système profondément technique et sophistiqué assure une expérience fluide aux utilisateurs, comme le doivent les offres destinées aux entreprises. »

**Kailash Nadh**  
Chief Technology Officer, Zerodha

Cloudflare Workers a changé la donne pour LendingTree. Nous pouvons exécuter du code JavaScript de manière asynchrone au sein d'une session client ou en parallèle de celle-ci, manipuler des données et prendre des décisions sans nuire aux performances ou à la disponibilité. Aucune autre solution ne propose cette fonctionnalité. »

**John Turner**  
Application Security Lead, LendingTree

« La plateforme Zero Trust de Cloudflare nous permet d'accorder à chaque collaborateur un accès basé sur le principe du moindre privilège à l'application dont il a besoin pour travailler. »

**Edward Fretwell**  
Engineering Director, Moneybox

Découvrez le premier cloud de connectivité cloud au monde. 

1. Grabner, Andreas. « Study: Silos Are the Chief Impediment to IT and Business Value » (Étude : les ressources cloisonnées constituent l'obstacle principal à la réalisation de la valeur en matière d'informatique et d'entreprise), The New Stack, 5 février 2021. <https://thenewstack.io/study-silos-are-chief-impediment-to-it-and-business-value/>
2. « New research shows CIOs need greater cross-team collaboration to drive digital transformation » (Une nouvelle étude montre que les DSI ont besoin d'une plus grande collaboration interéquipes pour conduire la transformation numérique), Dynatrace, 19 janvier 2021. <https://www.dynatrace.com/news/press-release/new-research-shows-cios-need-greater-cross-team-collaboration-to-drive-digital-transformation/>
3. « Gartner Survey Reveals 47% of Digital Workers Struggle to Find the Information Needed to Effectively Perform their Jobs » (Une étude Gartner révèle que 47 % des travailleurs du numérique ont du mal à trouver les informations dont ils ont besoin pour assurer efficacement leurs fonctions), Gartner.com, 10 mai 2023. <https://www.gartner.com/en/newsroom/press-releases/2023-05-10-gartner-survey-reveals-47-percent-of-digital-workers-struggle-to-find-the-information-needed-to-effectively-perform-their-jobs>
4. « The Economist Impact, une enquête approfondie et commandée par SAS, réalisée auprès de plus de 500 dirigeants du secteur bancaire en mars 2022 ». <https://impact-stage.economist.com/impact/banking-in-2035-global-banking-survey-report>
5. « Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024 » (Gartner révèle ses huit principales prédictions en matière de cybersécurité pour l'exercice 2023-2024), Gartner.com, 28 mars 2023. <https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024>
6. « Digital-first economy introduces unforeseen risks for 89% of CISOs » (L'économie axée sur le numérique introduit des risques pour 89 % des RSSI), Security Magazine, 20 juin 2023. <https://www.securitymagazine.com/articles/99528-digital-first-economy-introduces-unforeseen-risks-for-89-of-cisos>
7. En septembre 2023, Cloudflare a demandé à Forrester Consulting d'évaluer l'écosystème des solutions informatiques et de sécurité. Forrester a réalisé une enquête en ligne auprès de 449 décideurs informatiques en Amérique du Nord, en Europe, dans la région APAC et en Amérique latine.

© 2024 Cloudflare, Inc. Tous droits réservés.  
Le logo de Cloudflare est une marque commerciale de Cloudflare.  
Tous les autres noms de sociétés et de produits peuvent être des  
marques commerciales des sociétés auxquelles ils sont associés.

Téléphone : +33 7 57 90 52 73  
E-mail : [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com)  
Site : [www.cloudflare.com/fr-fr/](https://www.cloudflare.com/fr-fr/)