



# IBM Cloud for Financial Services

Accélérer l'innovation tout en répondant à vos  
besoins de sécurité et de conformité

## Un secteur en plein tumulte

Le secteur des services financiers doit faire face à de nombreux éléments perturbateurs, notamment des exigences toujours plus fortes de la part des clients pour des services innovants et personnalisés ; une concurrence intense des entreprises de technologie, technologies financières et titulaires ; une pression réglementaire toujours plus vive ; des menaces de cybersécurité en hausse ; et les besoins en employés qualifiés à même de gérer tous ces éléments.

Pour innover plus rapidement et se transformer, nombre d'institutions financières se tournent vers le cloud pour les aider à moderniser les applications existantes. Cela apporte davantage de souplesse et d'agilité, et permet de s'associer à des éditeurs de logiciels indépendants, fournisseurs de logiciels en tant que services (SaaS) et entreprises de technologies financières. L'exploitation optimale des technologies cloud permet aux institutions financières de remodeler leur expérience client, de rationaliser leurs opérations et d'envisager la définition de nouveaux modèles de recettes.

Toutefois, IBM a noté que beaucoup d'institutions financières ont retardé le passage de leurs charges de travail principales et de leurs données sensibles vers le cloud en raison du risque phénoménal lié à la cybersécurité et des difficultés réglementaires croissantes. Selon un rapport parrainé par IBM Security, le coût moyen d'une méga-violation des services financiers était de 401 millions de dollars (USD) en 2021 et le coût moyen d'une violation de données a augmenté de 10 % de 2020 à 2021.<sup>1</sup> Les compromis sur la sécurité ou la conformité réglementaire ne sont tout simplement pas acceptables.

Pour assurer leur compétitivité, les institutions financières devraient poursuivre le déplacement des charges de travail principales vers le cloud pour accélérer la transformation numérique et réduire leurs coûts, tout en maintenant la sécurité et la conformité de leurs données sensibles et de leurs charges de travail stratégiques. Pour ce faire, les institutions financières ont besoin d'un cloud basé sur les capacités spécifiques de sécurité et de conformité réglementaire dont ce secteur a besoin.

Les institutions financières ont besoin d'une option proposant le déplacement de leurs charges de travail et applications vers le cloud en toute transparence et, avec IBM Cloud for Financial Services™, le cloud public devient une alternative de plus en plus stratégique pour une accélération efficace de la transformation numérique.

## Un cloud développé pour le secteur

IBM Cloud for Financial Services est un cloud public unique en son genre, développé pour le secteur avec les capacités de sécurité et de contrôle qui aident les clients dans leur travail sur la minimisation des risques et l'accélération de l'adoption du cloud, mais également dans leurs charges de travail les plus sensibles.

Notre cloud est conçu pour aider les clients à automatiser leur position de sécurité et de conformité et à la surveiller grâce à la sécurité et aux contrôles intégrés à la plateforme, qui ne sont pas considérés comme des outils complémentaires ou des fonctionnalités à « bricoler ». En plus de capacités de sécurité et de confidentialité leaders du secteur, il est renforcé par IBM, sa connaissance approfondie en opérations informatiques, son expertise dans le secteur et son ensemble étendu de partenaires d'écosystème triés sur le volet.

Le résultat obtenu est un environnement sécurisé conçu pour aider les clients à faire baisser le risque et les coûts liés au déplacement des données sensible vers le cloud, à la modernisation des charges de travail et à l'intégration rapide des capacités nécessaires pour faire progresser leur activité.

Les institutions financières peuvent désormais profiter du cloud public tout en respectant leurs exigences de cybersécurité et de conformité réglementaire. Elles n'ont plus à choisir entre innovation et gestion des risques.

### Accélérer l'innovation, minimiser les risques

Premier cloud conçu en collaboration avec le secteur, IBM Cloud for Financial Services est conçu pour accélérer les innovations et contribuer à réduire les risques et les coûts de déplacement des données vers le cloud.



Gérez vos exigences de conformité avec une plateforme de contrôles communs conçue par le secteur.



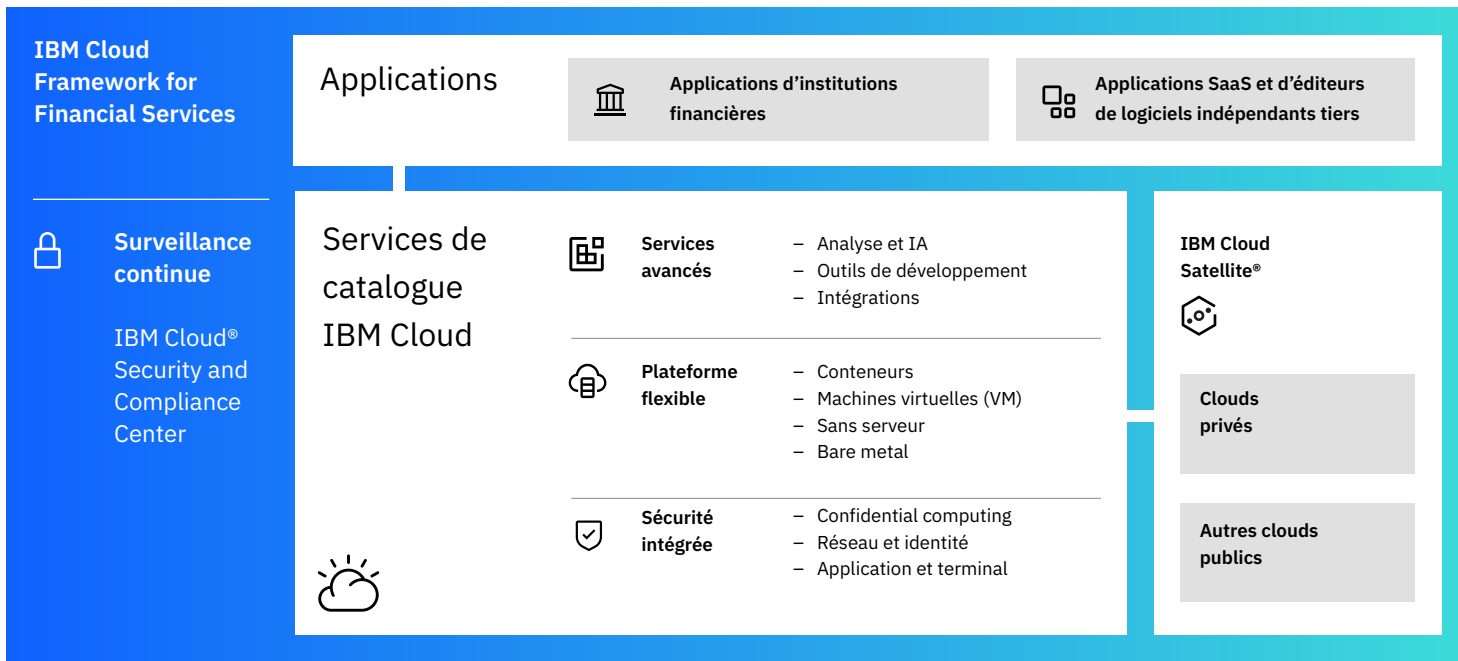
Accélérez l'innovation avec un écosystème d'éditeurs de logiciels indépendants, d'entreprises de technologies financières et de fournisseurs SaaS.



Assurez la sauvegarde de vos données avec des capacités de sécurité leaders du secteur.



Réalisez vos opérations avec agilité et en ayant le choix grâce aux options de déploiement de cloud hybride.



IBM Cloud for Financial Services exploite un cadre conseillé par le secteur avec des contrôles et une sécurité préconfigurés qu'IBM applique par programmation aux services IBM Cloud, aux applications tierces et aux charges de travail institutionnelles.

## Le cadre de contrôles : cœur de notre plateforme

Le cœur de notre offre est un cadre de contrôles appelé IBM Cloud Framework for Financial Services. Ce cadre a été développé pour aider les institutions financières à automatiser leur position de sécurité et de conformité afin qu'il soit plus facile, pour elles et leurs partenaires de la chaîne d'approvisionnement numérique, de gérer les risques et de démontrer leur conformité réglementaire.

Le cadre de contrôles offre une structure de sécurité et de conformité pour l'ensemble de l'écosystème grâce à un jeu commun de contrôles automatisés et préconfigurés appliqué aux services IBM Cloud®, applications tierces et charges de travail d'institutions financières. Créés en collaboration avec les principales institutions financières, les contrôles sont alignés sur les normes du secteur et les exigences des organismes de réglementation mondiaux. Ce cadre est validé en continu avec les conseils de l'IBM Financial Services Cloud Council, composé des DSI, directeurs techniques, RSSI et directeurs de la conformité et de la gestion des risques travaillant dans les plus grandes institutions financières, ainsi qu'avec les directives du Promontory Financial Group®, une société IBM et un leader mondial du conseil en conformité réglementaire. Le cadre évolue et les contrôles sont adaptés aux exigences et obligations réglementaires nouvelles du secteur pour aider les institutions financières dans leur réduction des coûts et de la complexité qu'impliquent un paysage réglementaire et de cybersécurité en évolution constante. Le jeu de contrôles étendu de l'IBM Cloud Framework for Financial Services comprend, entre autres éléments, la sécurité, la confidentialité des données, la gestion des accès et la gestion des configurations.

## Contrôles complets alignés sur les normes du secteur et les réglementations mondiales

7

Domaines de concentration

- Conformité et gestion des risques recentrées
- Protection avancée des données
- Authentification et gestion des accès améliorées
- Application automatisée et protection de la charge de travail
- Résilience et sécurité d'infrastructure unifiée
- Excellence opérationnelle
- Surveillance active des réponses

Au mois d'avril 2022

21

Familles de contrôles uniques

280

Contrôles

565

Exigences de contrôles

[En savoir plus sur IBM Cloud Framework for Financial Services →](#)

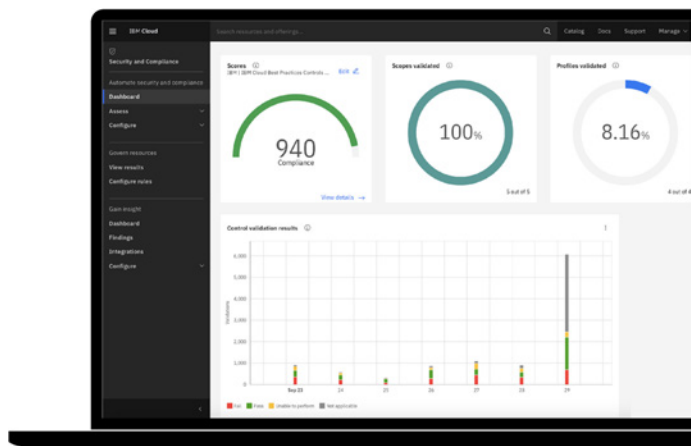
# Un riche catalogue d'éditeurs de logiciels indépendants, d'entreprises de technologies financières et de solutions SaaS

IBM Cloud for Financial Services est soutenu par un écosystème d'éditeurs de logiciels indépendants, d'entreprises de technologies financières et de fournisseurs SaaS triés sur le volet pour que les institutions financières puissent plus facilement et plus rapidement intégrer des applications et services tiers pour commencer à travailler ensemble sur notre cloud.

Grâce à l'IBM Cloud® Security and Compliance Center, les positions de sécurité et de conformité des applications et services partenaires peuvent être automatisées, surveillées en continu et exposées. Il en découle que les étapes manuelles du processus de gestion de la conformité pour les applications partenaires peuvent être réduites, que le potentiel d'erreur humaine peut être amoindri et que la cohérence, la traçabilité, l'auditabilité et l'évolution peuvent toutes être améliorées. Avec l'automatisation, les organisations sont également en mesure de réduire la variabilité entre les audits, ce qui génère des rapports aussi précieux que cohérents et supprime les retards tout en maintenant une conformité homogène.

## IBM Cloud Security and Compliance Center

L'IBM Cloud Security and Compliance Center contribue à aider les clients à surveiller et appliquer leurs contrôles dans le but de protéger les données et les actifs ainsi que de gérer les vulnérabilités dans les environnements cloud. Afin que les institutions financières puissent surveiller la position de sécurité et de conformité de leurs services cloud, en plus des applications et services partenaires, IBM fournit la plateforme et le tableau de bord de sécurité et de conformité dans le cadre d'un compte IBM Cloud. Les clients et les partenaires peuvent définir des profils de conformité, gérer les contrôles et maintenir un traçage des données extensible pour l'audit. Ceci contribue à la promotion d'une culture de conformité dans l'organisation, qui commence par la configuration des ressources et se maintient dans la collecte de preuves d'audit.



IBM Cloud Security and Compliance Center

L'intégration récente de Tanium Comply dans l'IBM Cloud Security and Compliance Center permet aux clients ayant des charges de travail régulées d'approfondir leur expérience en ayant la possibilité de visualiser les résultats d'évaluation de conformité de Tanium directement depuis l'IBM Cloud Security and Compliance Center. Avec Tanium Comply, les clients peuvent afficher leurs données de conformité associées au cloud IBM et à Tanium dans un même format, au même endroit. L'intégration de Tanium permet aux clients IBM Cloud d'étendre les capacités de gestion des terminaux de leurs organisations et d'inclure la recherche de vulnérabilités et de problèmes de configuration en fonction des normes de sécurité et des vulnérabilités du secteur.

## Sécurité et contrôles de protection des données leaders du secteur, avec approche Zero Trust

IBM Cloud for Financial Services a été conçu pour répondre aux besoins exigeants des organisations les plus grandes et les plus complexes. Il s'appuie sur les capacités et services de sécurité de protection des données intégrées au cloud public IBM, permettant ainsi une prise en charge des travaux stratégiques et des données hautement sensibles. IBM propose un cloud public de niveau entreprise avec des options étendues de déploiement, notamment VMware et Red Hat® OpenShift® en tant que service, et équipé pour répondre aux besoins spécifiques des services financiers.

IBM Cloud for Financial Services comprend des technologies de base pour la gestion des risques de sécurité et de la conformité réglementaire avec une approche centrée données à vérification systématique.

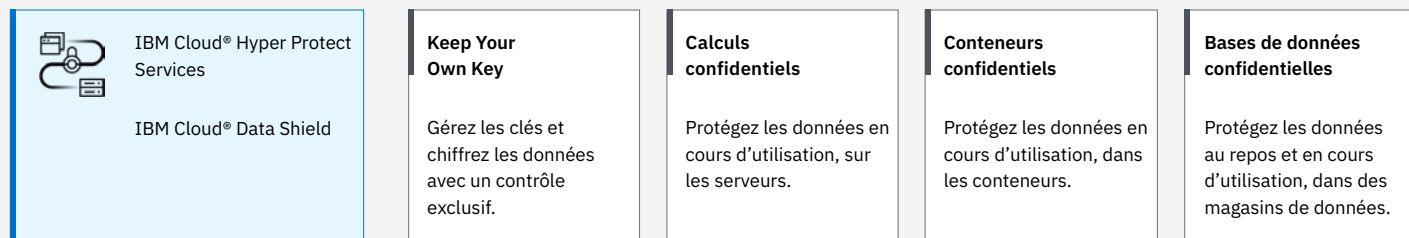
### Confidential computing

IBM adopte une approche globale du confidential computing, portant sur les calculs, les conteneurs, les bases de données et le chiffrement. Le confidential computing aide les clients à supprimer la confiance implicite que les applications accordent à la pile logicielle sous-jacente et aux fournisseurs cloud, de sorte que vous pouvez passer de mesures opérationnelles à des mesures techniques et protéger la confidentialité de vos données sensibles au repos, en transit ou en cours d'utilisation. Cela peut permettre aux clients de déplacer les données sensibles et les charges de travail vers le cloud, ouvrant la voie à de nouveaux modes de collaboration et d'innovation. Même s'il est impossible d'empêcher complètement les violations de données dans l'environnement de cloud hybride connecté actuel, une approche centrée données à vérification systématique peut aider les institutions financières à moderniser leurs opérations et à intégrer les contrôles de sécurité, en plus d'être conçue pour limiter l'impact et le coût d'une violation de données.

# Zero Trust : sécurité intégrée sur le réseau, l'identité, les terminaux et les applications

## Confidential computing par IBM : une approche globale pour protéger les données en transit, au repos et en cours d'utilisation

### Technologies et capacités permises



### Chiffrement de bout en bout avec contrôles étendus

Notre cloud de services financiers propose également une approche de gestion des clés leader du secteur qui apporte techniquement aux clients un contrôle exclusif sur leurs données. Même IBM ne peut pas y accéder.<sup>2</sup> IBM Cloud® Hyper Protect Crypto Services permet le chiffrement de données cloud dans un module de sécurité matérielle (HSM) cloud dédié. Le service propose des technologies telles que la conservation de votre propre clé (Keep Your Own Key - KYOK). Il s'agit d'un service de gestion des clés à locataire unique qui dispose de la protection des clés en coffre-fort fournie par des HSM dédiés et contrôlés par les utilisateurs, conçu pour accepter les normes de chiffrement du secteur comme la norme PKCS #11 (norme de cryptographie de clé publique). Il s'agit également du seul service cloud du secteur basé sur du matériel certifié FIPS 140-2 niveau 4. À ce niveau de sécurité, les mécanismes de sécurité physiques peuvent apporter une enveloppe de protection autour du module cryptographique dans le but de détecter et de répondre aux tentatives non autorisées d'accès physique.

Avec ce type de protection des données, le client est le seul parti à régir et contrôler l'accès à ses données privées. Ces capacités peuvent réellement changer la donne pour le secteur des services financiers qui doit respecter des exigences réglementaires strictes en matière de protection des données.

IBM Cloud for Financial Services fait appel à des services supplémentaires intégrés au cloud public IBM qui permettent également une utilisation pour les charges de travail stratégiques et les données sensibles.

### Sécurité axée par défaut sur les charges de travail

Chaque charge de travail a besoin de règles d'accès et de sécurité différentes. IBM permet aux organisations de définir et de faire appliquer de telles directives au moyen de la sécurité de conteneur intégrée et de DevSecOps pour les applications cloud natives avec Red Hat OpenShift en tant que service.

### Régions multizones (MZR)

Les clients peuvent exploiter les capacités sous-jacentes d'IBM Cloud for Financial Services pour améliorer la résilience



métier et la reprise après incident. Les MZR sont composées de zones de disponibilité interconnectées à grande vitesse et faible latence, indépendantes les unes des autres, pour contribuer à limiter l'impact des événements isolés à une seule et unique zone de disponibilité. Elles permettent aux institutions financières de placer les charges de travail dans des zones géographiques spécifiques en fonction de leurs besoins.

### Règles de journalisation et d'audit

Les fournisseurs SaaS et les éditeurs de logiciels indépendants ont pour obligation de journaliser toutes les actions effectuées dans le portail du cloud, l'API ou l'interface de ligne de commande afin qu'elles soient enregistrées en détail à l'aide d'IBM Cloud® Activity Tracker. Ce modèle permet une journalisation standard de l'activité sur les systèmes et services, ainsi qu'un enregistrement de sessions complètes des actions exactes entreprises par les opérateurs. Ces informations sont enregistrées et analysées de manière centralisée. Le processus de journalisation peut faire l'objet d'audits pour permettre le traçage de toutes les étapes, y compris la journalisation des événements ayant réussi ou échoué, et il confère une protection basée sur les rôles pour tous les points d'intervention. Les journaux d'accès sont stockés avec les horodatages pour aider à l'analyse et aux mesures légales.

# Moderniser et transformer une entreprise plus rapidement avec IBM Cloud for Financial Services

Pour aider les clients à moderniser et transformer leur activité plus rapidement avec IBM Cloud for Financial Services, IBM rejoint les clients « là où ils se trouvent » sur le parcours de l'adoption cloud en gérant les cas d'utilisation les plus importants pour eux, notamment :

- Prise en charge de la conformité réglementaire dans les charges de travail et les données des chaînes d'approvisionnement internes et numériques
- Protection des données sensibles dans le cloud avec une approche centrée données à vérification systématique (Zero Trust)
- Migration sécurisée des charges de travail virtualisées dans le cloud
- Développement et gestion sécurisés des applications cloud natives en conteneurs

Discutez avec votre représentant IBM et réalisez notre évaluation de contrôles gratuite pour comprendre où les technologies ainsi que le cadre de contrôle de sécurité de votre institution financière se placent par rapport à IBM Cloud Framework for Financial Services. Pour en savoir plus et accéder à des ressources supplémentaires, rendez-vous sur la [page Web IBM Cloud for Financial Services](#).

## Notes finales

1. *Cost of a Data Breach Report 2021*, IBM Security and Ponemon Institute, juillet 2021. <https://www.ibm.com/fr-fr/downloads/cas/OJDVQGRY>
2. D'après IBM Hyper Protect Crypto Services, le seul service cloud du secteur basé sur du matériel certifié FIPS 140-2 niveau 4. À ce niveau de sécurité, les mécanismes de sécurité physiques peuvent apporter une enveloppe de protection autour du module cryptographique dans le but de détecter et de répondre aux tentatives non autorisées d'accès physique.

© Copyright IBM Corporation 2022

Compagnie IBM France  
17 avenue de l'Europe  
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique  
Juillet 2022

IBM, le logo IBM, IBM Cloud for Financial Services, IBM Cloud, IBM Cloud Satellite et Promontory Financial Group sont des marques ou des marques déposées d'International Business Machines Corporation, aux États-Unis et/ou dans d'autres pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques d'IBM est disponible sur [ibm.com/trademark](http://ibm.com/trademark).

VMware est une marque déposée ou une marque commerciale de VMware, Inc. ou de ses filiales aux États-Unis et/ou dans d'autres juridictions.

Red Hat et OpenShift sont des marques ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

L'information contenue dans ce document était à jour à la date de sa publication initiale et peut être modifiée sans préavis par IBM. Les offres mentionnées dans le présent document ne sont pas toutes disponibles dans tous les pays où la société IBM est présente.

Il incombe à l'utilisateur d'évaluer et de vérifier le fonctionnement de tout autre produit ou programme avec les produits et programmes IBM. LES INFORMATIONS CONTENUES DANS LE PRÉSENT DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT SANS AUCUNE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER NI AUCUNE GARANTIE OU CONDITION D'ABSENCE DE CONTREFAÇON. Les produits IBM sont garantis conformément aux dispositions des contrats qui régissent leur utilisation.

Énoncé des bonnes pratiques de sécurité : La sécurité du système informatique implique la protection des systèmes et des informations par la prévention, la détection et la réponse à un accès inapproprié à l'intérieur et à l'extérieur de votre entreprise. Un accès inadapté peut entraîner la modification, la destruction, l'appropriation illicite ou l'utilisation abusive des informations ou peut entraîner des dommages ou une mauvaise utilisation de vos systèmes, y compris pour des attaques sur des tiers. Aucun système ou produit informatique ne doit être considéré comme totalement sécurisé et aucun produit, service ou mesure de sécurité ne peut être totalement efficace pour empêcher une utilisation ou un accès inapproprié. Les systèmes, produits et services d'IBM sont conçus pour faire partie d'une approche de sécurité légale et complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent exiger que d'autres systèmes, produits ou services soient plus efficaces. IBM NE GARANTIT PAS QUE LES SYSTÈMES, PRODUITS OU SERVICES SONT À L'ABRI DE, OU PROTÈGENT VOTRE SOCIÉTÉ CONTRE, LA CONDUITE MALVEILLANTE OU ILLÉGALE DE QUELQUE PARTIE QUE CE SOIT.

Il incombe au client de respecter les lois et règlements qui lui sont applicables. IBM ne fournit pas de conseils juridiques et ne déclare ni ne garantit que ses services ou produits garantiront que le client est en conformité avec toute loi ou réglementation. Les déclarations concernant les orientations et les intentions futures d'IBM sont susceptibles d'être modifiées ou retirées sans préavis et ne représentent que des buts et des objectifs.

