Sortir du brouillard :

Principales considérations pour la migration des paiements vers le nuage

CGI

La réalisation du plein potentiel de l'infonuagique, privé ou public, est attrayante pour les banques, mais il s'agit souvent d'un processus très complexe.

La solution CGI All Payments a aidé de nombreuses banques à surmonter cette complexité, à faire face aux risques et à fournir des solutions hautement résilientes et accessibles pour le traitement des paiements.

Introduction

Les arguments incitant les banques à remplacer leurs centres de traitement de données par une solution en nuage sont convaincants. Les avantages potentiels sont le développement durable, l'élasticité des ressources, la réduction de la planification de la capacité, l'accroissement de la résilience et de l'efficacité, ainsi que la diminution des coûts.

Ces nombreux avantages expliquent pourquoi, parmi les 311 dirigeants du secteur bancaire que nous avons interrogés dans le cadre de notre programme La voix de nos clients CGI 2024, 61 % prévoient la migration d'au moins 20 % de leurs principales applications d'affaires vers le nuage au cours des deux prochaines années.

Même si plusieurs banques considèrent que le nuage privé présente moins de risques de sécurité, la plupart d'entre elles ont hésité à transférer leurs systèmes centraux dans le nuage public en raison des défis de sécurité qui lui sont propres. La sécurité est essentielle pour les banques, car les ensembles de données qu'elles traitent sont constitués presque en totalité de renseignements permettant d'identifier une personne, et les conséquences de toute compromission sur le plan de la réglementation et de la réputation sont considérables. Pourtant, plus de 84 % des clients de CGI utilisent des solutions infonuagiques, telles que CGI All Payments, dont le profil de risque est inférieur à celui de leur ancienne infrastructure.

La protection des actifs essentiels est l'une des nombreuses préoccupations des banques lors de leur migration vers le nuage public. Elles ont aussi des obligations juridiques et réglementaires à respecter pour assurer la sécurité.

Il est évident que la migration de vos opérations de paiement vers le nuage public représente un défi et peut sembler insurmontable, c'est pourquoi nous souhaitons vous faciliter la tâche.

Chez CGI, nous aidons nos clients à mener à bien des projets complexes avec succès depuis de nombreuses années, qu'il s'agisse de commander des satellites au moyen de protocoles sécurisés, de transmettre des données importantes aux organismes de défense, de traiter les demandes de passeport ou de mettre en œuvre des systèmes de paiement de pointe.

Nos plus récents déploiements en matière de services de paiement ont impliqué l'utilisation de nuages privés et publics ainsi que des modèles hybrides. Trois capacités fondamentales ont aidé nos clients à surmonter les obstacles qui freinent habituellement d'autres entreprises.

1 **Plateforme**
Une plateforme de paiement adaptée aux besoins, indépendante du nuage et conçue pour les environnements à nuages multiples.

2 **Expérience**
Une vaste expérience de la gestion des infrastructures et des applications.

3 **Sécurité et résilience**
Une sécurité infonuagique avancée jumelée à une approche robuste en matière de gestion des risques.

En combinant ces trois capacités, nos clients ont migré leurs systèmes de paiement vers le nuage public de façon sécuritaire et transparente, réalisant ainsi la véritable promesse de l'infrastructure infonuagique.

La bonne plateforme

Le déploiement d'applications dans le nuage public présente un défi de taille, car il faut s'assurer que l'ensemble de la pile technologique permettra une mise en œuvre efficace et sécurisée.

Bien qu'il soit techniquement possible de migrer les applications d'un ordinateur central vers le nuage, cette approche est généralement évitée. Les applications d'un ordinateur central ne sont pas conçues pour le nuage ou pour en exploiter les avantages, ce qui rend ces migrations peu pratiques et potentiellement contre-productives.

Lorsque vous envisagez de migrer votre infrastructure de paiement vers le nuage public, la première étape consiste à trouver la plateforme la mieux adaptée. Cette solution polyvalente et évolutive, à la fois indépendante du nuage et conçue pour les environnements à nuages multiples, permet de tirer le meilleur parti des avantages du déploiement infonuagique. L'indépendance est un élément important de la réduction des risques liés à l'informatique en nuage. Bien que les fournisseurs de services en nuage se soient efforcés de rendre le déploiement plus accessible en proposant des outils conçus pour le nuage, l'utilisation de ces derniers empêche l'interopérabilité de la solution déployée. Elle peut également lier une banque à une plateforme infonuagique particulière et générer une dette technologique inhérente (c.-à-d. les coûts associés à la mise à niveau de technologies vieillissantes), c'est pourquoi nous travaillons en partenariat avec tous les principaux fournisseurs à grande échelle, parallèlement à l'utilisation d'outils infonuagiques.

Avant de déployer notre premier client dans le nuage public en 2019, nous avons réimaginé et conçu notre plateforme de paiements, CGI All Payments, pour répondre précisément à ces exigences. Fondée sur une structure de données conforme à la norme ISO 20022, la plateforme est conçue pour l'orchestration, le traitement en temps réel et les passerelles réseau certifiées. Elle permet également de traiter tout type de paiement, à toute heure du jour ou de la nuit.

L'intégration à CGI All Payments de ces capacités à l'épreuve du temps nous permet d'offrir des services de déploiement en nuage public et privé depuis plus de cinq ans, et d'aider nos clients à tirer parti de l'élasticité des ressources du nuage, de sa résilience, de sa grande disponibilité et de ses autres avantages.

Cette mesure est devenue extrêmement importante à l'heure où le traitement des paiements subit d'importants changements à l'échelle mondiale. D'ici l'an prochain, les infrastructures internationales de paiement auront adopté la norme ISO 20022 et pratiquement toutes les banques du monde devront offrir des services de paiement fondés sur cette norme. Les services régionaux, nationaux et transfrontaliers de paiement en temps réel et accessibles en tout temps sont déjà une réalité pour certaines banques, et elles commencent à reconnaître la nécessité de s'y préparer. De plus, l'infrastructure de paiement doit être plus flexible que les applications sur ordinateur central et prendre en charge un déploiement et une maintenance sécuritaires à distance, des besoins qui sont encore plus pressants depuis l'éclosion de la pandémie.

L'expérience pertinente

Bien qu'il est essentiel de trouver la bonne plateforme pour bénéficier des avantages du déploiement sur le nuage public,

le simple fait d'utiliser cette bonne plateforme ne suffit pas si les banques ne s'appuient pas sur une expérience pertinente pour déployer leurs systèmes de façon sécuritaire dans un environnement infonuagique résilient qui se répare automatiquement. Une expertise et des processus éprouvés en matière d'informatique en nuage, associés à une gestion efficace des risques liés au nuage, sont tout aussi essentiels pour réduire les risques, les coûts et les perturbations de l'activité que de choisir la plateforme et la solution de paiement adéquates.

Par l'entremise de nos services de conseil, nous effectuons une analyse approfondie des exigences (l'évaluation des risques liés au nuage de CGI) avant tout déploiement vers le nuage public afin de définir le pourquoi, le quoi, le quand et le comment du projet de migration. Cette analyse facilite la résolution proactive des problèmes, l'efficacité et la réduction des risques. Pour que cette analyse soit fructueuse, il faut communiquer clairement et ouvertement à propos des exigences, des enjeux, des occasions, des possibilités, etc. C'est pourquoi il est essentiel d'établir avec ses partenaires une relation de confiance, fondée sur l'honnêteté et la collaboration étroite.

Nous avons mis au point des processus robustes dans le nuage et avons investi de manière significative dans la formation et la certification du personnel afin d'aider les banques à mettre en œuvre ces processus. Nous offrons aux équipes des formations sur le fonctionnement de la plateforme déployée, sur la surveillance proactive et sur le dépannage et la résolution de problèmes, ou nous en assurons la gestion en leur nom. Ces processus de gestion sont rigoureusement mis à l'essai et, une fois opérationnels, hautement efficaces.

Nous avons été le premier partenaire mondial de transformation de Scaled Agile (SAFe). Cette approche de développement et de mise en œuvre nous a permis de réduire les délais de mise sur le marché tout en augmentant la qualité.

Puisque nos équipes agiles utilisent différents environnements lors du développement du code (p. ex. hors production, mise à l'essai, préproduction et production), elles sont en mesure de déployer une quantité moindre de code pour chaque version et de faire des mises à l'essai plus rapides et efficaces. De plus, grâce aux mises à l'essai automatisées, les équipes peuvent s'assurer que les changements requis n'ont aucune répercussion négative sur le code qui fonctionne déjà.

Nous déployons les applications dans des environnements entièrement adaptés aux besoins et qui utilisent les fonctionnalités du nuage public, telles que l'application automatisée de correctifs et la réparation automatique de Kubernetes, afin d'offrir un traitement en tout temps et une disponibilité surpassant grandement celle des déploiements traditionnels.

Tandis que la résilience du nuage rend le basculement moins probable, l'automatisation des processus réduit considérablement le temps de récupération en cas de défaillance de la géolocalisation à moins de 30 minutes. Nous réunissons ces atouts grâce à nos décennies d'expérience en prestation de services d'application en mode délégué auprès de clients du monde entier. Pour offrir ces services, nous appliquons le principe de droit d'accès minimal et limitons l'accès au personnel ayant obtenu les autorisations de sécurité nécessaires, établissons des ententes de niveau de service transparentes, employons des processus de gouvernance à la fois robustes et simples, et assurons une gestion du changement hautement efficace. Ces mesures assurent une grande efficacité, un faible coût et une grande qualité. De plus, tous nos services sont bien documentés et vérifiables, ce qui rassure les organismes de réglementation du secteur bancaire lorsqu'ils évaluent les ententes de service externes des banques.

Une sécurité et une résilience appropriées

La sécurité et la résilience représentent déjà un besoin essentiel pour toute infrastructure de paiement, car elles pourraient potentiellement anéantir l'économie en cas de violation ou de défaillance majeure.

Cependant, lorsque le traitement est migré vers le nuage public et qu'il contient des renseignements personnels et des données de paiement, une couche de protection supplémentaire est nécessaire. Comme c'est le cas pour l'introduction de toute technologie, les organisations doivent bien comprendre les risques réels et perçus, faute de quoi les organismes de réglementation et les responsables de la sécurité et de la résilience au sein des banques considèrent la démarche comme très risquée, malgré les retours évidents et les contrôles améliorés qui auront été mis en place.

Bien que les principaux fournisseurs de services infonuagiques publics, comme Microsoft Azure, Amazon Web Services et Google Cloud Platform, aient investi massivement dans la sécurité et la résilience, le renforcement d'un environnement particulier incombe à l'organisation responsable du déploiement. Les contrôles de sécurité en nuage doivent être mis en place et utilisés correctement pour assurer une sécurité efficace et éviter la création de vulnérabilités.

Par ailleurs, la résilience des données et des applications est essentielle pour assurer la disponibilité des systèmes de paiement, et il est primordial de savoir comment en tirer le meilleur parti.

Sur le plan de la sécurité, il est important de tirer parti de plusieurs outils de sécurité capables de surveiller automatiquement toutes les couches de protection, d'analyser le code source, de détecter la présence de vulnérabilités connues dans les produits tiers et de valider la configuration de l'environnement d'exécution. Cette mesure permet de réduire le risque continu lié à toute nouvelle vulnérabilité provoquée par des modifications de code, la configuration de l'environnement et des logiciels tiers. Notre approche globale de sécurité maintient un juste équilibre entre les risques de sécurité, l'incidence des contrôles de sécurité sur la productivité et les coûts associés à leur gestion.

La modélisation des menaces par arbres d'attaques (analyse des menaces), qui permettent de détecter les vecteurs d'attaque potentiels, est un outil nécessaire à la sécurité du nuage public. Cette modélisation permet d'aborder certaines grandes préoccupations des banques en matière de sécurité,

Exploitation de la surface d'attaque étendue pour effectuer un paiement frauduleux ou obtenir les données des clients :

Ce type d'attaque peut être mené par les employés d'une banque qui ont accès aux systèmes de traitement des paiements et, dans une certaine mesure, par les employés du fournisseur de services en nuage de la banque. Les principaux contrôles de sécurité permettant de prévenir ces attaques sont les suivants :

- **authentification multifacteur** pour tous les types d'accès (p. ex. utilisateurs, administrateurs);
- **cryptographie** afin de protéger les données de paiements à plusieurs niveaux (p. ex. chiffrement des données au repos et en mouvement, signatures numériques);
- **séparation** des fonctions du personnel;
- utilisation de registres de conteneurs privés **continuellement analysés** et **restriction de l'accès Internet** à partir des environnements d'exécution.

Exploitation de la surface d'attaque étendue pour causer une interruption de service :

Les principaux contrôles de sécurité permettant de prévenir ces attaques sont le verrouillage du réseau, la protection contre les attaques par déni de service distribué, le ralentissement artificiel du trafic et la restriction de l'accès aux utilisateurs essentiels. Lors d'un déploiement de nuage hybride, l'accès peut être restreint à l'aide d'un réseau privé virtuel (RPV) ou d'un RPV de site à site entre tous les sites (p. ex. ceux du fournisseur de services en nuage et de la banque). Il peut également être restreint au moyen d'hôtes bastion (ou « jump server »), de serveurs de gestion et d'une infrastructure de bureau virtuel sans installer de logiciels.

Cette approche permet d'intégrer la sécurité, et non de l'ajouter, de sorte que le risque de ne pas détecter une vulnérabilité ou d'en créer une par erreur est réduit.

Nous savons que la sécurité n'est pas uniquement une question de technologie, mais qu'elle concerne aussi les processus et les personnes. La mise en œuvre d'une approche exhaustive et de processus éprouvés contribue à la sensibilisation des personnes, ce qui réduit les vecteurs d'attaque potentiels.

Sur le plan de la résilience, nous tirons parti de la puissance inhérente du nuage pour passer de l'ancienne idée « active:active » à « self-healing:active:hot:warm » (autorétablissement, active, chaude, tiède), en veillant essentiellement à ce que la production ne faiblisse que rarement, que les basculements nécessaires en cas de catastrophe puissent être effectués de façon transparente et avec une redondance suffisante pour garantir un retour rapide aux opérations en cas de failles liées à la cybersécurité ou à la mise à jour des outils. Ce changement de modèle, combiné à une solide posture de sécurité, complète la justification du passage à l'infonuagique en offrant une résilience qui dépasse les capacités des infrastructures traditionnelles, comme l'ordinateur central.

Réunir tous les éléments

Depuis plus de cinq ans, nos clients de ce segment traitent les paiements au moyen de CGI All Payments, notre solution en nuage public approuvée par les organismes réglementaires. En collaborant étroitement avec nos clients, nous avons pu résoudre des problèmes complexes liés à l'informatique en nuage et aider des banques avant-gardistes à se tourner vers le développement durable, la réduction des coûts, le renforcement de la sécurité et vers une meilleure exploitation de leurs ressources.

Les succès de nos clients reposent sur la combinaison des composantes appropriées, de l'expertise pertinente et de l'atténuation des risques potentiels. De plus, nos activités ont permis la réalisation d'une exécution reproductible. Conformément aux tendances du marché illustrées par notre étude La voix de nos clients, nous prévoyons que le déploiement d'une infrastructure de paiement dans le nuage public deviendra la norme au cours des prochaines années.

C'est le moment idéal pour envisager de travailler avec CGI afin de profiter des avantages d'un déploiement en nuage public ou privé. Nous pouvons vous aider à atteindre vos objectifs, quel que soit le service infonuagique que vous choisissez.

Pour en savoir davantage, visitez CGI.com ou écrivez-nous à info@cgi.com. Nous serons heureux de discuter de votre stratégie de migration vers le nuage.

À propos de CGI

Allier savoir et faire

Fondée en 1976, CGI est l'une des plus importantes entreprises de services-conseils en TI et en management au monde.

Nous sommes guidés par les faits et axés sur les résultats afin d'accélérer le rendement de vos investissements. À partir de centaines de bureaux à l'échelle mondiale, nous offrons des services-conseils complets, adaptables et durables en TI et en management. Ces services s'appuient sur des analyses mondiales et sont mis en œuvre à l'échelle locale.

cgi.com