Migrer les paiements vers le nuage public grâce à CGI All Payments

La promesse du nuage, qu'il soit privé ou public, est alléchante pour les banques. Parmi ses nombreux avantages figurent notamment son caractère écoresponsable, l'élasticité des ressources, la réduction des tâches de planification de la capacité, l'accroissement de la résilience et de l'efficacité, et la diminution des coûts.

Les arguments incitant les banques à remplacer leurs centres de traitement de données par une solution en nuage sont donc convaincants. D'ailleurs, 60 % des 264 dirigeants du secteur bancaire que nous avons interrogés dans le cadre de notre programme La voix de nos clients 2021 prévoient de migrer au moins 21 % de leurs applications vers le nuage au cours des deux prochaines années.

Cependant, compte tenu du fait que certains ensembles de données sont composés presque exclusivement de renseignements permettant d'identifier une personne et des conséquences potentielles d'une intrusion, la sécurité est un enjeu majeur pour les banques. Nombreuses d'entre elles perçoivent le nuage privé comme une option moins risquée, mais la plupart hésitent à migrer leurs systèmes de base – ou les « joyaux de la couronne », comme les appelle l'un de nos clients – vers le nuage public en raison de ses défis uniques en matière de sécurité.

Toutefois, la protection de leurs principaux actifs n'est pas la seule préoccupation des banques en ce qui a trait à la migration vers le nuage public. Elles ont aussi des obligations juridiques et réglementaires à respecter pour assurer la sécurité. En raison de ces défis, la démarche de migration des paiements vers le nuage public peut sembler très complexe, voire intimidante.

Chez CGI, nous aidons nos clients à aborder les situations 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 de façon novatrice ou de mettre en œuvre des systèmes de paiement de pointe. Lors de nos plus récents projets de déploiement des paiements vers des nuages privés et publics, nous avons constaté que les trois capacités fondamentales ci-dessous aident nos clients à surmonter les obstacles qui freinent les progrès de leurs concurrents.

Plateforme

Plateforme de paiements adaptée au projet, conçue pour les environnements à nuages multiples et compatible avec différents nuages

Expérience

Longue expérience en gestion d'infrastructures et d'applications

Sécurité

Sécurité infonuagique avancée, jumelée à une approche rigoureuse de gestion des risques

Il n'est pas excessivement complexe de mettre en œuvre ces capacités fondamentales de façon isolée, mais il faut faire preuve d'une concentration et d'un dévouement absolus pour les réunir. En conjuguant ces trois capacités, nos clients ont été en mesure de migrer leurs services de paiement vers le nuage public de façon sécuritaire et transparente.

La bonne plateforme

Pour migrer une application vers le nuage public, il faut d'abord s'assurer que l'ensemble de la pile technologique de l'application puisse être déployée de façon efficace et sécuritaire. Bien qu'il existe des technologies pour migrer les applications sur ordinateur central vers le nuage, rares sont les organisations qui choisissent cette option puisque ces applications ne sont pas conçues pour être hébergées dans le nuage ni pour tirer parti de ses avantages.

Lorsqu'une banque envisage la possibilité de migrer son infrastructure de paiement vers le nuage public, la première étape consiste à trouver une plateforme à la fois adaptée aux besoins du projet, conçue pour les environnements à nuages multiples et compatible avec différents nuages, qui leur permettra de tirer pleinement profit du déploiement en nuage. La compatibilité avec différentes technologies est importante pour réduire les risques associés au nuage. Bien que les fournisseurs de nuage s'efforcent de faciliter le déploiement en proposant des outils conçus spécialement pour le nuage, leur utilisation nuit à l'interopérabilité de la solution déployée, peut rendre une banque dépendante à une plateforme infonuagique particulière, et génère une dette technologique inhérente (c.-à-d. les coûts associés à la mise à niveau de technologies vieillissantes).

En 2016, nous avons commencé à repenser et refondre notre plateforme de paiements, CGI All Payments, afin de satisfaire ces exigences précises. Fondée sur une structure de données conforme à ISO 20022, notre plateforme est spécialement conçue pour offrir des capacités d'orchestration, un traitement en temps réel et des 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 a permis d'offrir des services de déploiement en nuage public et privé plus rapidement que nos concurrents, 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.

En cette période de transition majeure du marché mondial du traitement des paiements, le choix de la plateforme est devenu extrêmement important. D'ici cinq ans, 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 internationaux de paiement en temps réel et accessibles en tout temps sont déjà une réalité pour certaines, et les banques sont conscientes de la nécessité de s'y préparer. De plus, l'infrastructure de paiement devra 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 mondiale.

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 la 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.

Pour minimiser les risques, les coûts et les répercussions sur les activités, il est tout aussi important de se doter d’une expertise et de processus infonuagiques éprouvés ainsi que de capacités efficaces de gestion des risques.

Par l’entremise de nos services-conseils, 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. Cet exercice 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 important d’établir avec ses partenaires une relation de confiance, fondée sur l’honnêteté et la collaboration étroite.

Pour ce qui est de l’exécution, nous avons développé des processus infonuagiques robustes et avons fortement investi dans la formation et la certification du personnel afin d’aider les banques durant la mise en œuvre. Nous offrons à leurs équipes des formations sur le fonctionnement de la plateforme déployée, sur la surveillance proactive et sur le dépannage et la résolution de problèmes. Ces processus de gestion sont rigoureusement testés et, une fois opérationnels, hautement efficaces.

En 2019, nous sommes devenus 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, test, 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 à des mises à l’essai automatisées, elles peuvent s’assurer que les changements à apporter n’auront aucune incidence négative sur du code déjà fonctionnel.

Les applications sont déployées dans un environnement entièrement adapté aux besoins et 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. Non seulement la résilience du nuage rend les interruptions de service moins probables, mais l'automatisation des processus réduit aussi à moins de 30 minutes le temps de rétablissement après un échec de géolocalisation.

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 méthodes favorisent l'efficacité, l'abordabilité et la 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.

Les mesures de sécurité appropriées

La sécurité représente déjà une nécessité pour toute infrastructure de paiement, puisque ces infrastructures gèrent généralement des données qui ont le potentiel de paralyser l'économie en cas d'intrusion. Cependant, lorsque des renseignements permettant d'identifier une personne sont migrés vers le nuage public et contiennent des données de paiement, il faut ajouter une couche de protection supplémentaire. 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 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 nuages publics comme Microsoft Azure, Amazon AWS et Google Cloud aient investi massivement dans la sécurité, la tâche de renforcer un environnement précis appartient à l'organisation responsable du déploiement. Pour assurer une sécurité efficace et éviter la création de vulnérabilités, il faut mettre en place des contrôles de

sécurité infonuagiques et les utiliser correctement. Les contrôles tels que le cadre NIST 800 et le cadre de contrôle de la sécurité des clients sont essentiels pour sécuriser le déploiement des services de paiement, et il est primordial de savoir comment bien les mettre en application.

Il est aussi important de tirer parti d'outils de sécurité appropriés qui surveillent automatiquement toutes les couches de protection, analysent le code source, détectent la présence de vulnérabilités dans les produits tiers, et valident la configuration de l'environnement opérationnel. Ces mesures permettent de minimiser le risque constant d'introduire de nouvelles vulnérabilités en modifiant le code, en configurant l'environnement ou en déployant des logiciels tiers.

La mise en œuvre et la gestion de certains contrôles de sécurité peuvent être très coûteuses même s'ils ne contribuent que très peu à l'atténuation des risques. 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.

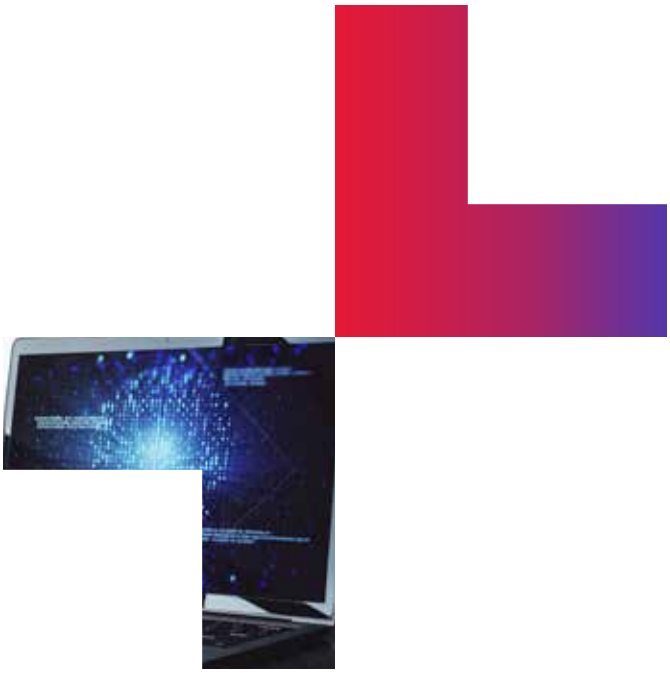
Les arbres d'attaques (un modèle pour l'analyse des menaces), qui permettent de détecter les vecteurs d'attaque potentiels, sont un outil nécessaire pour la sécurité infonuagique. Ce modèle permet d'aborder certaines grandes préoccupations des banques en matière de sécurité.

Exploitation de la surface d'attaque étendue pour effectuer un paiement frauduleux ou obtenir les données des clients – Ce type d'attaque peut non seulement être mené par les employés d'une banque qui ont accès aux systèmes de traitement des paiements, mais aussi, dans une certaine mesure, par les employés du fournisseur de services infonuagiques 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., cryptage 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 « serveurs jump »), de serveurs de gestion et d'une infrastructure de bureau virtuel sans installer de logiciels.

Notre approche comprend tout le nécessaire pour assurer l'efficacité des contrôles de sécurité. Grâce à cette approche, nous intégrons la sécurité à tous les processus dès le début du projet plutôt que de la greffer



au système peu avant la date de lancement, ce qui réduit le risque d'omettre une vulnérabilité ou d'en créer une par erreur.

Nous savons que la sécurité n'est pas uniquement une question de technologie, mais qu'elle concerne aussi les processus et les personnes. Ces dernières sont souvent le maillon le plus faible du processus de sécurité. La mise en œuvre d'une approche exhaustive et de processus éprouvés contribue à la sensibilisation des personnes, ce qui réduit par le fait même les vecteurs d'attaque potentiels.

De plus, la création d'une politique fondée sur le principe de droit d'accès minimal est une arme efficace contre les violations internes et externes. La réalisation d'une enquête de sécurité pour l'ensemble du personnel ajoute également une autre couche de protection contre les vulnérabilités et constitue un excellent complément à toutes les autres mesures de sécurité.

Réunir tous les éléments

Comme peuvent en témoigner nos clients qui ont migré leurs systèmes et qui traitent maintenant les paiements au moyen de notre solution en nuage public approuvée par les organismes réglementaires, notre approche rassemble tous les éléments essentiels au succès. En collaborant étroitement avec eux, nous avons pu résoudre des problèmes complexes et aider des banques avant-gardistes à adopter cette option écoresponsable, à réduire les coûts et à optimiser l'exploitation de leurs ressources.

Le succès de nos clients repose sur la combinaison des composantes appropriées, d'une expertise pertinente et de l'atténuation des risques potentiels. Nos projets nous ont également permis de créer une procédure d'exécution reproductible. Nous nous attendons à ce que le déploiement des infrastructures de paiement sur le nuage public devienne la norme d'ici environ un an.

C'est le moment idéal d'envisager une collaboration avec CGI pour 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 sites 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