NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

En quoi le cloud souverain et de confiance va-t-il pouvoir accélérer le passage au cloud dans le secteur bancaire ?

Résumé

- L'intégration du cloud dans le **très réglementé secteur bancaire** s'accélère à vitesse grand V, promettant d'importants **gains de compétitivité**.
- De **nombreux cas d'usages** se révèlent pertinents et prometteurs : déploiement d'applications accéléré, lien direct data/digital, amélioration des problèmes d'infrastructure...
- Les **réglementations** ne manquent pas : PCI DSS, RGPD, DORA, NIS2... à ce titre, le cloud souverain et de confiance se révèle être un **choix particulièrement judicieux**.

Une récente étude menée par Capgemini a montré une **accélération très forte du secteur bancaire** et assurance dans l'intégration du cloud dans ses opérations, avec un pourcentage d'intégration passant de 37% des répondants en 2020 à 91% en 2023.

En effet, le secteur bancaire et financier au sens large gérant avant tout de la **data**, l'enjeu y est principalement d'exploiter au mieux ce patrimoine **levier de compétitivité** majeur. Le cloud, par sa capacité à gérer des volumes de données à la demande, de stocker, de proposer des services à la demande.... est donc un vecteur de compétitivité indéniable.

Des cas d'usages et des fonctionnalités nombreuses

- Gommage des questions d'infrastructure au profit d'un focus métier
- Déploiement plus rapide des applications
- Mise à disposition de services et briques qui permettent d'innover par assemblage, en limitant les développements et en accélérant le time-to-market
- Lien direct entre data et digital qui s'enrichissent mutuellement et boostent l'innovation
- Accélération de l'innovation via notamment des usages avancés d'Analytics et de business intelligence
- Amélioration de la gestion client et prise en charge plus rapide des demandes grâce notamment à l'IA

Pourquoi les secteurs de la banque, finance et assurance peinent-ils à franchir le pas ?

L'étude de Capgemini fournit là encore une partie de la réponse. Parmi les défis qui entravent une adoption efficace du cloud à grand échelle, figure **la sécurité des données** qui est citée comme « un obstacle majeur » pour 68 % des dirigeants interrogés.

De nombreux défis à adresser en tête desquels la sécurité des données au sens large

Les établissements financiers et les assurances manipulent des données hautement sensibles, puisqu'il s'agit de données patrimoniales ou de santé qui sont des données particulièrement intimes. Ils ont des obligations règlementaires fortes de différentes natures, qu'ils maîtrisent la plupart du temps dans leurs systèmes on-premise.

L'offre de cloud public trustée jusqu'à présent par les hypersaclers ne garantit pas la **confidentialité des données**, et limite donc de facto les applications externalisées dans le cloud public.

En effet, les hyperscalers sont soumis aux lois américaines, le **Cloud Act** et le **Fisa**, qui autorisent le gouvernement américain à la réquisition des données sans obligation d'informations de quiconque. Les cloud provider sont d'ailleurs tenus de publier ces demandes de réquisitions sur leur site, Google par exemple a fait l'objet en 2022 de près de 500 demandes de réquisition, portant sur plus de 100 000 comptes utilisateurs.

Ainsi, en externalisant leurs applications ou opérations dans un cloud non souverain, cela supposerait des opérations et process additionnels de type pseudonymisation, voire anonymisation des données, validation des opérations par les DPO...qui rajouteraient de la complexité, pour un résultat relatif dans certains cas.

Prenons à ce titre l'exemple de l'IA. Pour se garantir la pleine performance des modèles, il est souvent préférable d'entraîner ces derniers sur les données d'origine, ce qui dans des cloud non souverains n'est pas possible. Donc le jeu n'en vaut donc pas toujours la chandelle.

Ainsi, les **nombreuses règlementations** auxquelles sont soumis les acteurs du secteur banque/finance (voir ci-après un extrait de ces règlementations) apparaissent souvent comme difficilement compatibles avec des cloud non souverains, car ne pouvant garantir la sécurité totale des données, les hyperscalers étant soumis aux lois américaines.

> **Voici un extrait des réglementations :**

> **PCI DSS**
PCI DSS est un ensemble de normes de sécurité regroupées en **12 exigences** conçues pour protéger les données des clients et les informations de paiement contre tout accès, utilisation ou divulgation non autorisés. La conformité à la norme PCI DSS est **obligatoire** pour toute entreprise qui traite, stocke ou transmet des informations relatives aux cartes de crédit.

- **Le RGPD**
  Le RGPD (Règlement Général sur la Protection des Données) est un cadre de sécurité conçu pour protéger les informations personnelles des citoyens et en garantir la confidentialité totale tout au long du cycle de vie. Toute entreprise qui traite des données à caractère personnel de citoyens de l'UE, que ce soit manuellement ou automatiquement, doit s'y conformer.

- **Le DORA**
  Le **DORA (Digital Operational Resilience Act)** a pour objectif d'améliorer la résilience opérationnelle informatique des acteurs des services financiers, en mettant en place un cadre de gouvernance et de contrôle interne spécifique. Dora s'inscrit dans le cadre plus large d'un train de mesures sur la finance numérique, qui vise à mettre au point une approche européenne favorisant le développement technologique et assurant la stabilité financière et la **protection des consommateurs**. L'un des principaux pans est d'**assurer la continuité d'activité en cas d'incident majeur**, ou de sinistre, en évaluant principalement la capacité des établissements à mettre en place un plan de continuité au niveau des principales activités financières. Dans ce cadre, le recours à un cloud souverain et de confiance qualifié SecNumCloud (le plus haut standard de sécurité français), permet de faciliter une **mise en conformité au règlement Dora**.

- **NIS2**
  NIS2 (Network and Information System), adopté par le Parlement et le Conseil de l'Union Européenne le 14 décembre 2022 remplace et abroge la directive NIS1.

  Il a pour objectif le renforcement de la cybersécurité des réseaux et des systèmes d'information au sein de l'Union Européenne et impose ainsi des obligations minimales en matière de cybersécurité et de déclaration d'incidents aux opérateurs de services essentiels (OSE), aux fournisseurs de services numériques (FSD) mais également maintenant à toute entreprise employant plus de 250 personnes, dont le chiffre d'affaires annuel dépasse 50 millions d'euros et/ou dont le bilan annuel est supérieur à 43 millions d'euros. Là aussi, le recours à un cloud souverain et de confiance qualifié SecNumCloud (le plus haut standard de sécurité français) permet de faciliter une **mise en conformité au règlement NIS2**.

Le cloud souverain et de confiance, un accélérateur pour le passage au cloud du secteur

Un cloud dit souverain permet de :

- Se prémunir contre les risques géopolitiques qui pourraient conduire à une rupture de service par exemple et couper l'accès aux données.
- Ne pas être soumis aux lois extraterritoriales

Un cloud dit de confiance, à savoir qualifié SecNumCloud, le plus haut niveau de sécurité décerné par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Informations) permet :

- D'être en conformité de facto avec un certain nombre d'exigences règlementaires du secteur et de faciliter la mise en conformité
- De bénéficier d'un niveau de sécurité au plus haut niveau de maitrise décrit par les référentiels actuels

Ces alternatives souveraines et de confiance devraient donc **lever un certain nombre de réserves** de la part des acteurs du secteur. Le secteur bancaire a une forte culture du on-premise, le **cloud public** est donc souvent considéré comme un asset dans une stratégie de cloud hybride chère au secteur.

Néanmoins avec l'arrivée de **solutions publiques souveraines et de confiance**, de nouveaux pans d'activité comme les datas platform pourraient basculer dans le cloud et l'adoption du cloud s'accélérer notoirement.

Contactez-nous

Jean Atmé, Responsable Secteur Banque et Assurance
jean.atme@numspot.com

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous

@NumSpot
@NumSpotCloud