# MIGRER SEREINEMENT VERS LE CLOUD AVEC SPIE ICS

**Une migration Cloud raisonnée et sereine exige un plan et une boussole. SPIE ICS recommande d'envisager cinq stratégies, de segmenter ses workloads et de contrôler les accès aux données.**

Les facteurs clés d'une migration Cloud réussie débutent par une démarche structurée, l'apprentissage de nouvelles pratiques, DevOps et FinOps notamment, et des prérequis organisationnels et techniques. Chaque application et son infrastructure sous-jacente doit être étudiée, sa mise en œuvre soigneusement planifiée, pour bâtir un Cloud efficace, sûr et accessible, sans dépendance vis-à-vis des fournisseurs.

Que l'on souhaite améliorer la reprise d'activités après un sinistre, externaliser des applications ou innover autour de technologies d'IA pour rester compétitif, ce sont les cas d'usage qui guident les managers. Il s'agit de fixer des objectifs clairs, en intégrant chacun des services (DSI, achats, RH et métiers), au sein de la DSI. SPIE ICS établit un état des lieux et implique toutes les parties prenantes concernées par cette transformation.

## Cinq approches envisageables

« Nos clients effectuent, en majorité, un Lift and Shift avant d'opérer une transformation vers une plateforme PaaS ou des logiciels SaaS. Les applications très structurantes comme l'ERP restent généralement hébergées sur le site de l'entreprise, tandis que d'autres applications sont déplacées vers une infrastructure de confiance, » observe **Hervé Grégoire, responsable du développement des offres Cloud de SPIE ICS**. Ce changement d'hébergement correspond au premier des cinq modèles à prendre en considération:

***L'approche Rehost*** (Lift and Shift) revient à déplacer une application existante vers le Cloud sans modifier son architecture, ni sa configuration. Cette stratégie est bien adaptée aux entreprises qui débutent leur transformation numérique et cherchent un Move To Cloud rapide avec le moins de perturbations possibles.

***L'approche Replatform*** (Lift and Reshape) implique une migration avec des transformations (PaaS par exemple), pour tirer parti des capacités natives du Cloud, comme l'intégration d'outils d'automatisation, ou l'amélioration du gestionnaire de données. L'entreprise gagne en flexibilité et en performance, sans avoir à refondre tout son site marchand par exemple ; elle s'assure qu'il gère plus efficacement les pics de trafic.

***L'approche Rearchitect*** consiste à repenser l'architecture d'applications monolithiques pour exploiter les avantages du Cloud, des micro-services et offrir une montée à l'échelle dynamique. Bien qu'elle exige de former et de coordonner les concepteurs, exploitants IT et la TMA, cette voie de migration s'avère plus agile et plus rentable à terme.

***L'approche Retain*** revient à conserver certaines applications sur site, souvent pour des raisons réglementaires ou financières. Elles ne sont pas migrées, mais peuvent être interfacées aux logiciels livrés en mode SaaS via un Cloud. Par exemple, l'entreprise conserve son système de gestion des transactions sur site pour respecter une conformité sectorielle, tandis qu'elle exploite le Cloud pour des analyses ponctuelles menées sur des échantillons de données anonymes.

***L'approche Retire*** vise à supprimer ou à remplacer les applications obsolètes. Cette rationalisation des workloads contribue à optimiser les ressources matérielles. Par exemple, un ancien SIRH est remplacé par une solution SaaS plus moderne, tandis que les données historiques nécessaires sont archivées.

### Gouvernance Cloud et améliorations continues

L'entreprise gagne à identifier ses workloads éligibles, à les segmenter, puis à garder le contrôle des accès pour savoir qui accède à quelles données, où et comment. Cette gouvernance est essentielle car les collaborateurs assurant eux-mêmes l'administration des partages ne sont pas à l'abri d'une surexposition d'informations. Du coup, l'acculturation de chacun à la cybersécurité devient incontournable. Une révision de la charte des usages, des guides de bonnes pratiques sécurisées, et une supervision des espaces partagés réduisent les risques de fuites de données sensibles.

**« Des améliorations continues deviennent possibles lorsqu'on suit le cycle itératif consistant à penser, concevoir, construire, puis exploiter son Cloud privé, public ou hybride. Nous déterminons avec les clients les SLA nécessaires, en termes de disponibilité de services et de sécurité, et fixons des engagements dès la migration, » précise Antonio Freitas, directeur technique de la BU Datacenter de SPIE ICS.**

L'entreprise peut ainsi choisir son cheminement vers le Cloud, et également prévoir un rapatriement en interne de ses workloads, pour quelque raison que ce soit.

### EN CAS DE CYBERATTAQUE, QUI SUPPORTE LE PRÉJUDICE SUBI ?

Les sociétés attaquées sont-elles en droit de se retourner contre leur prestataire d'infrastructure ?

Un fabricant de portails français a été victime, en juin 2020, d'un crypto-locker suite à une attaque par hameçonnage. Toutes ses données cruciales et l'intégralité de ses sauvegardes, toutes connectées, ont été chiffrées par l'attaquant. Cela a provoqué l'arrêt du SI durant une semaine, un manque à gagner significatif et une image de marque dégradée.

La cour de Rennes a rappelé l'article 1241 du Code civil : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »

En novembre 2024, la cour a estimé que l'absence de backup déconnecté formait un manquement à l'obligation de conseil du prestataire qui se targuait d'être expert en cybersécurité. Elle a requis à son encontre une indemnisation pour préjudice de l'ordre de 50 000 €, soit près d'un tiers du coût de la prestation qui aurait dû tenir compte des recommandations de l'ANSSI, résumées dans le guide d'hygiène informatique depuis 2017.

**Pour en savoir plus sur notre expertise Cloud**