# LAN (on-premise) vs Cloud

## I –Comparaison générale

|  |  |  |
| --- | --- | --- |
| Critère | LAN / On-Premise | Cloud (IaaS, PaaS, SaaS) |
| Contrôle | Contrôle total sur données, infrastructures, sécurité. | Contrôle partiel : dépendance au fournisseur (perte de souveraineté). |
| Coûts | Investissement initial élevé (CAPEX), coûts fixes. | Coûts variables (OPEX) mais imprévisibles à long terme, souvent plus élevés que prévu. |
| Scalabilité | Limitée : nécessite ajout physique de serveurs. | Élevée et quasi instantanée (auto-scaling). |
| Maintenance | Interne, maîtrisée mais coûteuse. | Externalisée (mise à jour automatique). |
| Disponibilité | Dépend de la redondance locale. | Très haute, mais dépend d’une connexion stable et du fournisseur. |
| Sécurité | Contrôlée localement, mais exige des compétences. | Mutualisée, standardisée, parfois vulnérable à des attaques ou erreurs de configuration. |
| Souveraineté / conformité | Données sous juridiction interne. | Risque de transfert vers des juridictions étrangères (Cloud Act, etc.). |
| Innovation / IA | Lente, limitée par les capacités internes. | Forte intégration d’IA, de services managés, de DevOps, etc. |

## II – Comparaison par typologie de cloud

**IaaS (Infrastructure as a Service)**

* **Avantages Cloud :**
  + Évite les investissements matériels lourds (serveurs, stockage).
  + Haute disponibilité, automatisation.
  + Facilité d’expérimentation (machines virtuelles élastiques).
* **Inconvénients Cloud :**
  + Coûts variables importants à long terme.
  + Dépendance au fournisseur (AWS, Azure, GCP).
  + Sortie de données (egress fees) coûteuse.
* **Raisons de rapatriement :**
  + Optimiser les coûts, reprendre le contrôle sur la performance et la sécurité.
  + Réduction de 30 à 50 % des dépenses selon Andreessen Horowitz (Dropbox, Basecamp).

**PaaS (Platform as a Service)**

* **Avantages Cloud :**
  + Environnement de développement rapide et flexible.
  + Gestion automatisée des mises à jour et de la montée en charge.
* **Inconvénients Cloud :**
  + Forte dépendance aux technologies du fournisseur.
  + Risque de verrouillage technologique (« vendor lock-in »).
  + Moins de personnalisation.
* **Raisons de retour au LAN / cloud privé :**
  + Difficulté d’intégration avec systèmes internes.
  + Nécessité de conformité stricte (secteurs finance, santé).
  + Mieux maîtriser les performances et la traçabilité.

**SaaS (Software as a Service)**

* **Avantages Cloud :**
  + Aucune maintenance locale.
  + Accessibilité mondiale (messagerie, CRM, ERP).
  + Idéal pour la collaboration et le télétravail.
* **Inconvénients Cloud :**
  + Données hébergées à l’extérieur.
  + Risque de fuites ou de pertes d’accès en cas de litige ou panne.
  + Difficulté d’export des données (portabilité limitée, dépendance juridique).
* **Raisons de réinternalisation :**
  + Volonté de souveraineté (RGPD, Cloud Act).
  + Sécurisation accrue de données sensibles.
  + Retour vers des solutions open source auto-hébergées (Nextcloud, OnlyOffice).

## III – Pourquoi les entreprises choisissent encore le Cloud

* **Agilité et innovation :**
  + L’IA, le big data, et la conteneurisation (Kubernetes) reposent sur des ressources cloud évolutives.
* **Réduction du temps de déploiement :**
  + Accès immédiat à des ressources et outils collaboratifs.
* **Compétitivité :**
  + L’investissement cloud est perçu comme un levier d’innovation par Gartner (2028 = bascule du cloud en “standard industriel”).
* **Résilience et continuité :**
  + Disponibilité mondiale, sauvegardes automatisées.
* **Modèle hybride et multicloud :**
  + Recherche d’équilibre : flexibilité du cloud + contrôle du LAN.

## IV – Pourquoi les entreprises réinternalisent (Cloud Repatriation)

**Principales causes :**

1. **Explosion des coûts non prévus :**
   1. Factures multipliées par 2,5 chez Geico.
   2. Imprévisibilité des dépenses selon Citrix et Basecamp.
2. **Complexité technique accrue :**
   1. Environnements cloud hétérogènes, intégrations difficiles.
3. **Sécurité et souveraineté :**
   1. Risques de violation de conformité, d’espionnage ou de perte de maîtrise (RGPD, NIS2, DORA).
4. **Performance et fiabilité :**
   1. Latence ou défaillance de services critiques (notamment en IA et calculs intensifs).
5. **Dépendance excessive à un fournisseur unique :**
   1. Stratégies « multicloud » et « cloud souverain » en forte hausse.

## V – Tendances actuelles

|  |  |
| --- | --- |
| Tendance 2025 | Description |
| Cloud hybride | Mélange cloud public / privé / on-premise, compromis coût-contrôle. |
| Multicloud | Diversification des fournisseurs pour éviter le verrouillage (VMware/Broadcom → Nutanix). |
| Cloud souverain européen | Alignement avec NIS2, DORA et Data Act pour assurer l’interopérabilité et la portabilité. |
| Rapatriement partiel | Réservation du cloud pour l’IA, mais retour sur site pour les données critiques. |

## VI. Management des risques : comprendre les évolutions possibles

### 1. Pourquoi raisonner en « risques » ?

Lorsqu’une entreprise choisit entre **héberger son système d’information en interne (LAN)** ou dans le **cloud**, elle doit réfléchir en termes de **risques**.

Un **risque**, c’est un **événement négatif possible** (ex. : panne, fuite de données, hausse de coûts) qui a :

* **une probabilité** de se produire (faible, moyenne ou forte),
* **un impact** sur l’entreprise (faible, moyen ou fort).

Le **management des risques** consiste donc à repérer ces menaces, à estimer leur gravité, puis à décider : faut-il les **accepter**, les **réduire**, les **transférer** (assurance) ou les **éviter** ?

### 2. Les grands types de risques selon l’hébergement

|  |  |  |
| --- | --- | --- |
| Type de risque | Hébergement interne (LAN) | Hébergement Cloud (IaaS, PaaS, SaaS) |
| Technique (pannes, sauvegardes, sécurité) | Risque de panne locale si les équipements tombent en panne ou ne sont pas redondés. | Moins de pannes graves, mais dépendance à la connexion Internet et au fournisseur. |
| Financier (coûts, investissement) | Gros investissements au départ (serveurs, maintenance). Coûts plus prévisibles. | Coûts mensuels variables : souplesse mais risque de facture trop élevée à long terme. |
| Juridique et souveraineté | Données stockées sur le territoire, sous lois françaises ou européennes. | Risque de dépendance à des acteurs soumis à des lois étrangères (ex. : Cloud Act américain). |
| Organisationnel (compétences, gestion) | Nécessite du personnel informatique qualifié et disponible. | Moins de techniciens internes, mais dépendance à un prestataire externe. |
| Stratégique (autonomie, pérennité) | Maîtrise totale des données et outils, mais innovation plus lente. | Innovation rapide, mais risque de verrouillage (« lock-in ») : difficile de changer de fournisseur. |

### 3. Évolution probable des risques dans les années à venir

**a. Facteurs géopolitiques et économiques**

* **Tensions internationales** : les conflits ou sanctions économiques peuvent perturber les grands acteurs du cloud (notamment américains).
* **Hausse du coût de l’énergie et du matériel** : impact sur le prix des abonnements cloud et sur les serveurs internes.
* **Fragmentation du numérique** : chaque région (Europe, États-Unis, Chine) développe ses propres règles, ce qui complique les transferts de données.

👉 **Conséquence :** les entreprises européennes cherchent à se tourner vers des **clouds souverains** (ex. : SecNumCloud) ou vers des solutions **hybrides** (mi-cloud, mi-interne).

**b. Facteurs juridiques et réglementaires**

* **NIS 2 et DORA** (textes européens en vigueur d’ici 2026) : imposent une meilleure gestion des incidents, des plans de continuité et la traçabilité des données.
* **Règlement sur les données (Data Act)** : oblige les fournisseurs de cloud à faciliter la **portabilité** (export des données).
* **RGPD** : toujours une contrainte forte sur la localisation et la protection des données personnelles.

👉 **Conséquence :** les entreprises devront prouver qu’elles **maîtrisent la sécurité et les transferts** de leurs données, quel que soit le lieu d’hébergement.

**c. Facteurs technologiques**

* **Intelligence artificielle** et **analyse massive de données** demandent beaucoup de puissance de calcul : cela pousse vers le cloud.
* Mais les coûts et la dépendance augmentent, ce qui conduit certaines entreprises à **rapatrier** une partie de leurs serveurs pour mieux contrôler leurs dépenses et leurs performances.
* L’avenir est donc **hybride** : les tâches exigeant de la puissance restent dans le cloud, les données sensibles reviennent en interne.

## 4. Lecture simple des probabilités et impacts

|  |  |  |  |
| --- | --- | --- | --- |
| Risque étudié | Probabilité à court terme | Impact potentiel | Niveau de vigilance |
| Hausse du coût du cloud | Forte | Élevé (baisse de rentabilité) | ⚠️ Surveiller les dépenses et prévoir un plan de sortie. |
| Panne locale sur LAN | Moyenne | Fort | ⚠️ Investir dans la redondance et un plan de secours (PRA). |
| Fuite ou perte de données sensibles | Moyenne à forte | Très fort | 🔴 Priorité absolue : sauvegardes, chiffrement, contrôles d’accès. |
| Non-conformité juridique (NIS2, RGPD) | Moyenne | Fort | ⚠️ Nommer un responsable conformité et vérifier les clauses contractuelles. |
| Verrouillage fournisseur (Cloud) | Forte | Fort | ⚠️ Prévoir des contrats réversibles et des formats ouverts. |
| Pénurie de compétences internes (LAN) | Moyenne | Moyen | ⚠️ Former ou mutualiser les ressources informatiques. |

## 5. Les scénarios possibles pour les entreprises

**🟢 1. Poursuivre vers le cloud**

* Pertinent pour les activités **internationales** ou à **forte variabilité** (pics de charge).
* Offre une **souplesse** et une **rapidité** d’innovation.
* Risque financier : à contrôler par un **suivi régulier des coûts** (FinOps).

**🟡 2. Rapatrier partiellement ses données (cloud hybride)**

* Conserve les **avantages du cloud** pour l’agilité et l’IA.
* Garde sur site les **données sensibles** ou les applications critiques.
* C’est aujourd’hui la **solution la plus équilibrée** selon la plupart des DSI.

**🔵 3. Revenir majoritairement en interne (on-premise)**

* Pertinent si les coûts cloud deviennent excessifs ou si les contraintes de souveraineté sont fortes (banques, santé, défense).
* Permet un **contrôle complet**, mais demande **investissement, compétences et sécurité renforcée**.