Sécurité On-Premise vs Cloud

1. Modèle de responsabilité

On-Premise

L'entreprise est responsable de l'ensemble de la chaîne :

- Sécurité physique du datacenter
- Réseau
- Serveurs
- Hyperviseur
- Systèmes d'exploitation
- Applications
- Données
- Sauvegardes
- PRA / PCA

Responsabilité : totalement interne.

Cloud

Fonctionnement selon un modèle de responsabilité partagée.

Couche	Fournisseur Cloud	Client
Datacenter	✅	❌
Matériel	✅	❌
Virtualisation	✅	❌
OS (IaaS)	✅	✅
Applications	✅	✅
Données	✅	✅
Configuration IAM	✅	✅

Le fournisseur sécurise l'infrastructure. Le client sécurise la configuration, les accès et les données.

---

2. Sécurité physique

On-Premise

- Contrôle d'accès aux locaux
- Vidéosurveillance
- Gestion des accès physiques
- Protection incendie
- Alimentation électrique redondée

Cloud

- Sécurité physique gérée par le fournisseur
- Datacenters certifiés (ISO 27001, SOC, etc.)
- Haut niveau de redondance et de protection

Avantage : niveau industriel difficilement atteignable pour une PME.

---

3. Gestion des identités et des accès (IAM)

On-Premise

- Active Directory local
- Gestion souvent plus statique
- Granularité parfois limitée

Cloud

- IAM très granulaire (policies, RBAC)
- Rôles temporaires
- MFA natif
- Fédération d’identités (SSO, SAML, OIDC)

Risque majeur en Cloud : mauvaise configuration des droits.

---

4. Surface d’attaque

On-Premise

- Infrastructure moins exposée par défaut
- Accès via VPN ou réseau interne

Cloud

- Ressources accessibles via Internet
- APIs exposées
- Risques de mauvaise configuration (ex : stockage public)

Le Cloud augmente la surface d’attaque logique.

---

5. Risque principal

On-Premise

- Failles techniques
- Correctifs non appliqués
- Obsolescence matérielle

Cloud

- Erreurs de configuration
- Rôles trop permissifs
- Mauvaise gestion des accès
- Exposition involontaire de données

En Cloud, la mauvaise configuration est un facteur de risque majeur.

---

6. Gestion des correctifs

On-Premise

- L'entreprise gère tous les correctifs
- Processus parfois lent

Cloud

Dépend du modèle :

- IaaS : le client gère l'OS
- PaaS : le fournisseur gère l'OS
- SaaS : le fournisseur gère l'ensemble

La charge de patch management peut être fortement réduite en PaaS/SaaS.

---

7. Scalabilité et élasticité

On-Premise

- Infrastructure relativement stable
- Capacité limitée

Cloud

- Création et suppression dynamique d’instances
- Infrastructure éphémère
- Infrastructure as Code

La sécurité doit être automatisée (approche DevSecOps).

---

8. Journalisation et supervision

On-Premise

- SIEM interne
- Centralisation parfois complexe

Cloud

- Journalisation native (CloudTrail, équivalents)
- Traçabilité complète des appels API
- Intégration facilitée avec SIEM

La visibilité est souvent meilleure en environnement Cloud.

---

9. Chiffrement

On-Premise

- Mise en œuvre manuelle
- HSM coûteux

Cloud

- Chiffrement natif au repos et en transit
- Services KMS managés
- Rotation automatisée possible

---

10. Conformité et certifications

On-Premise

- L’entreprise doit démontrer seule sa conformité

Cloud

- Certifications fournies par le fournisseur (ISO 27001, SOC, PCI-DSS, etc.)
- La conformité reste partagée

La responsabilité réglementaire n’est pas transférée au fournisseur.

Synthèse

Critère	On-Premise	Cloud
Responsabilité	Totale entreprise	Partagée
Sécurité physique	Interne	Fournisseur
IAM	Moins granulaire	Très granulaire
Risque principal	Faille technique	Mauvaise configuration
Patch management	Interne	Selon modèle
Scalabilité	Limitée	Élevée
Monitoring	Variable	Natif
Chiffrement	Complexe	Intégré

Message clé

En environnement On-Premise, le risque provient principalement de l’infrastructure. En environnement Cloud, le risque provient principalement de la configuration.

From:
http://slamwiki2.kobject.net/ - **SlamWiki 2.1**

Permanent link:
http://slamwiki2.kobject.net/eadl/bloc4/fm4/premise-vs-cloud?rev=1772292720

Last update: **2026/02/28 16:32**