



ARCHITECTURE CLOUD ET HYBRIDES



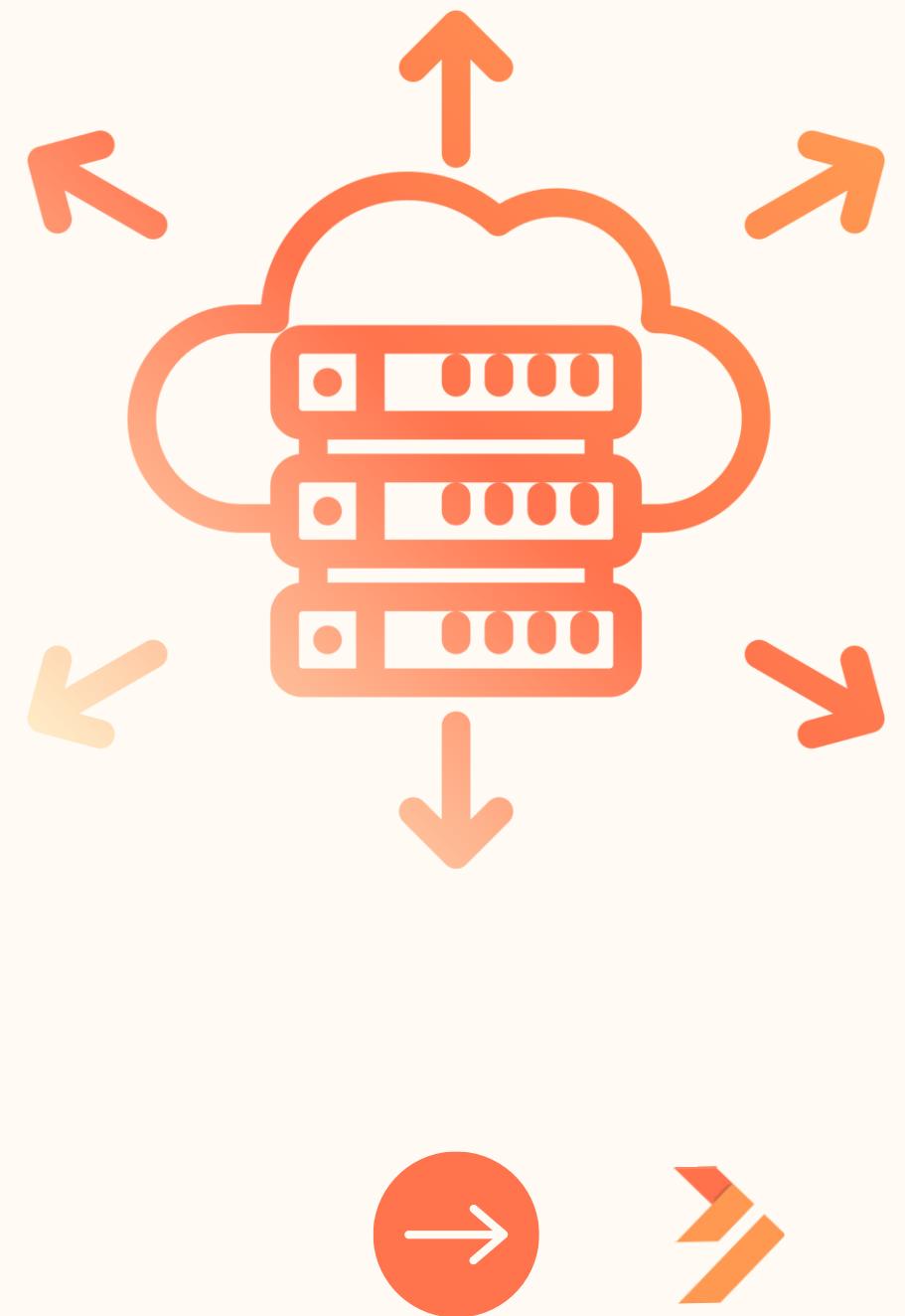
Intervenant : Nathan VIDAL FAGES





PRÉSENTATION DU MODULE

- Chapitre 1 : Introduction aux architectures Cloud et hybrides
- Chapitre 2 : Gestion des risques liés aux architectures Cloud et hybrides
- Chapitre 3 : Stratégies de protection des données en environnement Cloud
- Chapitre 4 : Stratégies de protection des applications en environnement Cloud
- Chapitre 5 : Mise en pratique à travers des études de cas





CHAPITRE 1:

INTRODUCTION AUX ARCHITECTURES CLOUD ET HYBRIDES





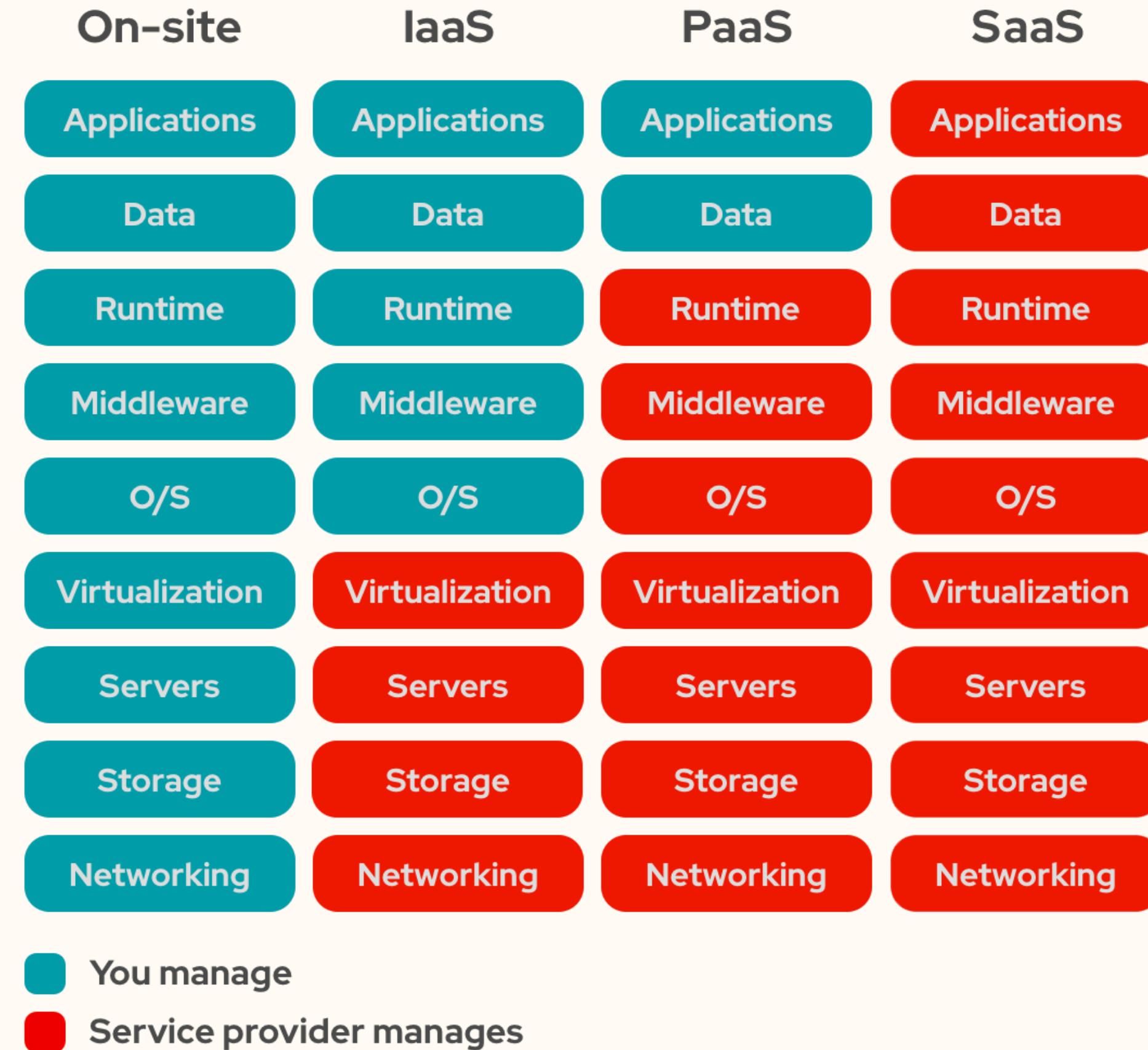
DÉFINITION DU CLOUD COMPUTING

MODÈLES DE
SERVICES





DÉFINITION DU CLOUD COMPUTING





EVERYTHING AS A SERVICE (XaaS)

- **DESKTOP AS A SERVICE (DaaS)**
Externalisation d'une solution VDI (Virtual Desktop Infrastructure) dans le Cloud, où l'utilisateur peut accéder directement à un bureau virtuel à distance (une session sur un système d'exploitation).
- **COMMUNICATIONS AS A SERVICE (CAAS)**
Modèle qui fait référence aux services de communication basés sur Internet (téléphonie par Internet, visioconférence, etc.)
- **DATABASE AS A SERVICE (DBAAS)**
Référence à la mise à disposition d'un système de bases de données via le Cloud
- **VPN AS A SERVICE (VPNAAS)**
Lorsque le VPN est proposé sous la forme d'un service
- **RANSOMWARE AS A SERVICE (RAAS)**
Référence à un modèle utilisé par les cybercriminels qui offrent la possibilité de louer un logiciel malveillant de type ransomware et toute l'infrastructure associée.

MODÈLES DE
SERVICES



MODÈLES DE DÉPLOIEMENT

➤ CLOUD PUBLIC

Ressources partagées, opérées par un fournisseur tiers (AWS, Azure, OVH).

➤ CLOUD PRIVÉ

Infrastructure dédiée, interne ou hébergée (VMware, OpenStack).

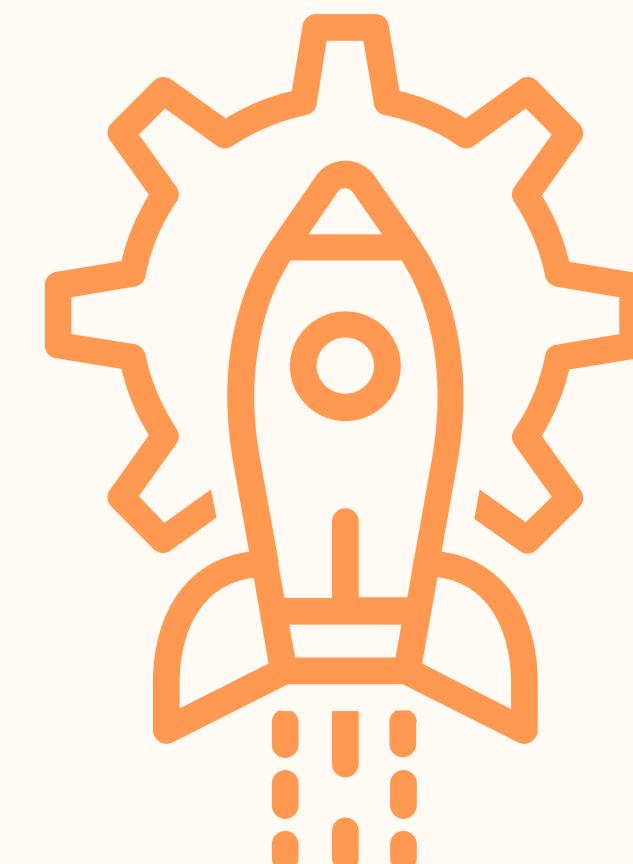
➤ CLOUD HYBRIDE

Combinaison des deux, permettant flexibilité et optimisation.

➤ MULTICLOUD

Utilisation de plusieurs fournisseurs pour éviter le verrouillage et augmenter la résilience.

MODÈLES DE SERVICES





CAS PRATIQUE

CARTE MENTALE AVANTAGES / DÉFIS



OBJECTIF

IDENTIFIER COLLECTIVEMENT LES AVANTAGES/DÉFIS DU CLOUD.

DÉROULÉ - GROUPES DE 5 ÉTUDIANTS

➤ SUR UNE FEUILLE / TABLEAU COLLABORATIF, DESSINER UNE CARTE AVEC DEUX BRANCHES :

AVANTAGES DU CLOUD

DÉFIS / RISQUES DU CLOUD

CHAQUE GROUPE DOIT TROUVER AU MOINS 5 AVANTAGES ET 5 DÉFIS.



**20
MIN**

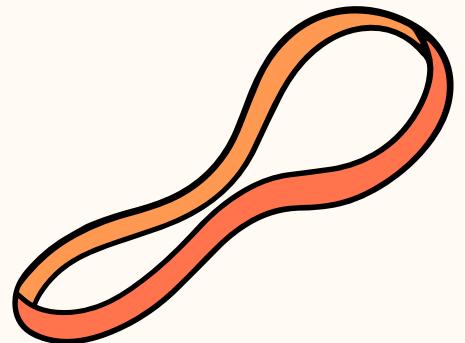
ANALYSE EN GROUPE

CHAQUE GROUPE PARTAGE 2 AVANTAGES + 2 DÉFIS → COMPIILATION EN TABLEAU
COMMUN

AVANTAGES ET DÉFIS DU CLOUD

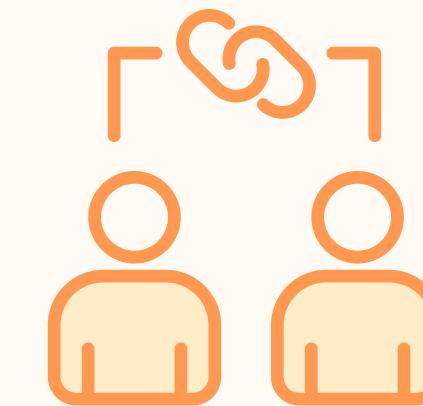
1

AVANTAGES



2

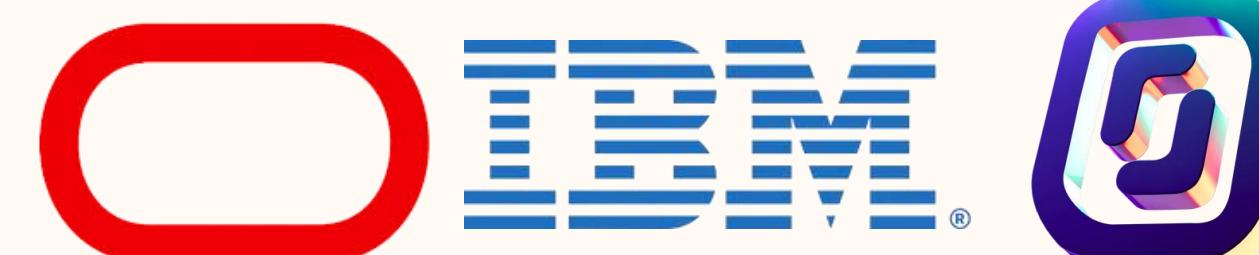
DÉFIS





LES GRANDS ACTEURS DU MARCHÉ

aws





ENJEUX DE SÉCURITÉ SPÉCIFIQUES



- MODÈLE DE RESPONSABILITÉ PARTAGÉE
 - FOURNISSEUR CLOUD
 - CLIENT

- PRINCIPAUX ENJEUX
 - PROTECTION DES DONNÉES
 - GESTION DES IDENTITÉS ET DES ACCÈS
 - SURVEILLANCE ET DÉTECTION
 - PLAN DE CONTINUITÉ ET REPRISE D'ACTIVITÉ



QUIZZ

VRAI / FAUX

- GOOGLE DRIVE EST UN SERVICE SAAS
- AMAZON EC2 EST UN SERVICE PAAS.
- LE CLOUD HYBRIDE COMBINE CLOUD PRIVÉ ET CLOUD PUBLIC.
- NETFLIX REPOSE SUR AWS.
- DROPBOX EST UN SERVICE IAAS.
- UN CLOUD PRIVÉ EST TOUJOURS PLUS SÉCURISÉ QU'UN CLOUD PUBLIC.

- AVEC LE CLOUD, LA SÉCURITÉ EST 100% GÉRÉE PAR LE FOURNISSEUR.
- MICROSOFT AZURE EST SURTOUT UTILISÉ POUR LES ENVIRONNEMENTS HYBRIDES.
- LE CLOUD SUPPRIME TOTALEMENT LE RISQUE DE PERTE DE DONNÉES.
- SPOTIFY EST UN EXEMPLE DE SAAS.
- LE MULTICLOUD CONSISTE À UTILISER PLUSIEURS FOURNISSEURS CLOUD POUR UN MÊME SI.
- SALESFORCE EST UN EXEMPLE DE PAAS

CONCLUSION

- LE CLOUD OFFRE DE NOMBREUX AVANTAGES MAIS NÉCESSITE UNE MAÎTRISE DES MODÈLES DE SERVICE ET DE DÉPLOIEMENT.
- LA SÉCURITÉ N'EST PAS EXTERNALISÉE : LE CLIENT CONSERVE DES RESPONSABILITÉS CLÉS.
- LA COMPRÉHENSION DE CES ENJEUX EST ESSENTIELLE AVANT D'ABORDER LA GESTION PROACTIVE DES RISQUES.



CHAPITRE 2:

GESTION DES RISQUES LIÉS AUX ARCHITECTURES CLOUD ET HYBRIDES





1. INTRODUCTION À LA GESTION DES RISQUES (CONCEPTS CLÉS)

DÉFINITION DU
RISQUE

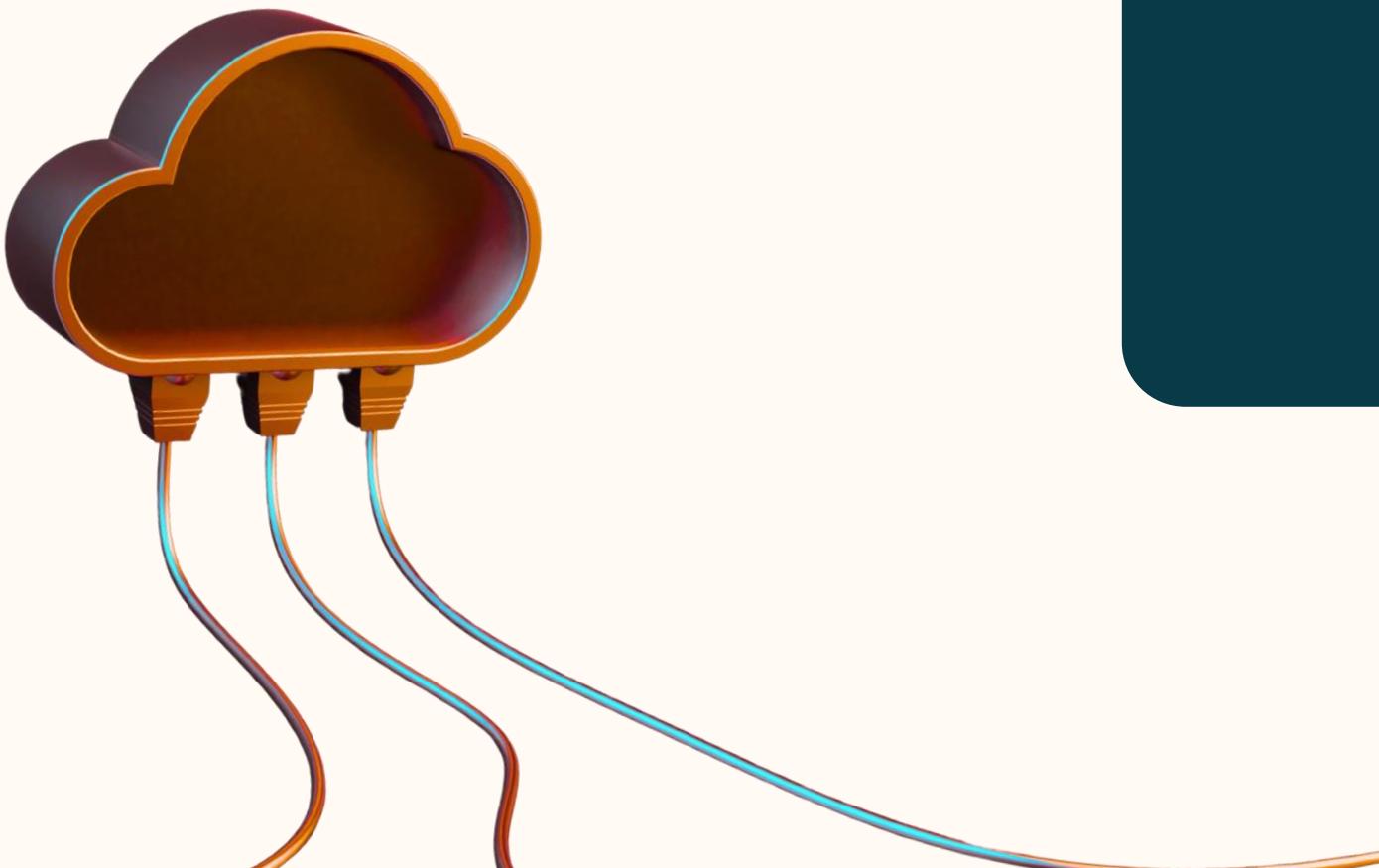
DIFFÉRENCES ENTRE
SI CLASSIQUE ET
SI CLOUD





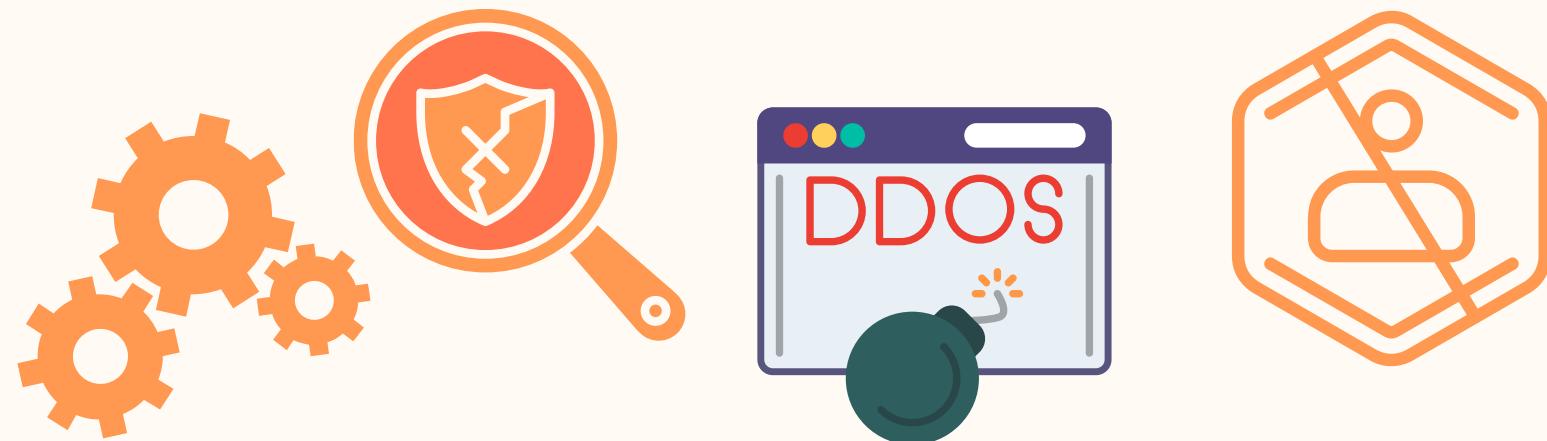
DÉFINITION DU
RISQUE

DIFFÉRENCES ENTRE
SI CLASSIQUE ET
SI CLOUD



2. TYPOLOGIE DES RISQUES SPÉCIFIQUES AU CLOUD

1 TECHNIQUES



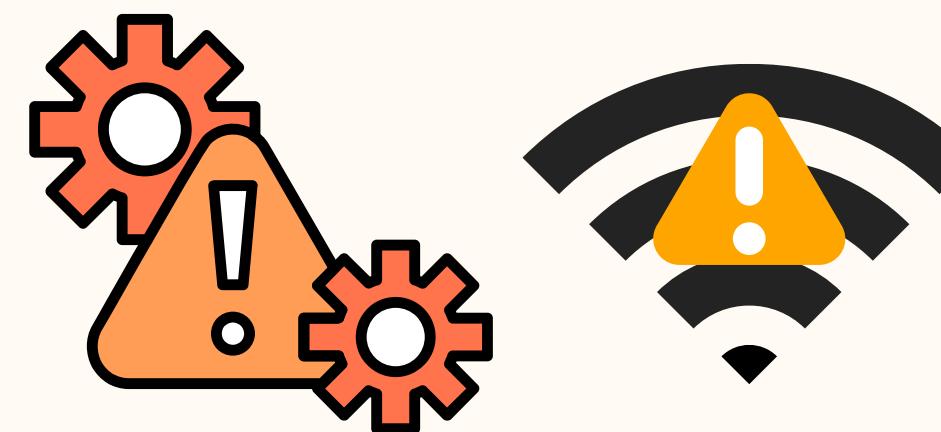
3 CONTRACTUELS / JURIDIQUE



2 ORGANISATIONNEL



4 OPÉRATIONNELS





3. ÉVALUATION DE L'IMPACT DES RISQUES

MÉTHODOLOGIE SIMPLE (UTILISABLE EN COURS)

- IDENTIFIER LES RISQUES.
- DÉTERMINER LEUR PROBABILITÉ (FAIBLE, MOYENNE, FORTE).
- DÉTERMINER LEUR IMPACT (FAIBLE, MOYEN, FORT).
- COMBINER POUR OBTENIR UN NIVEAU DE CRITICITÉ.

MÉTHODES AVANCÉES

- EBIOS RISK MANAGER (ANSSI) / ISO 27005 / FAIR



EXERCICE

MATRICE DE CRITICITÉ

OBJECTIF

- LISTE DE RISQUES : FUITE S3, PANNE AZURE RÉGIONALE, PIRATAGE COMPTE ADMIN, SHADOW IT, DDOS
- CHAQUE GROUPE DOIT PLACER CES RISQUES DANS UNE MATRICE 2x2 (PROBABILITÉ FAIBLE/FORTE × IMPACT FAIBLE/FORT).
- EXPLIQUER UN CHOIX “CRITIQUE” ET COMMENT Y RÉPONDRE.

LIVRABLE ATTENDU

- MATRICE DES RISQUES SUR FEUILLE / MAIL : esn@vidalfages.fr



40 MIN
ANALYSE EN
GROUPE



4. MESURES DE PRÉVENTION ET DE DÉTECTION

PRÉVENTION



DÉTECTION

CORRECTION
ET RÉPONSE



5. GOUVERNANCE ET CONFORMITÉ

➤ RÈGLEMENTATIONS



➤ NORMES & CERTIFICATIONS





ENJEUX DE SÉCURITÉ SPÉCIFIQUES

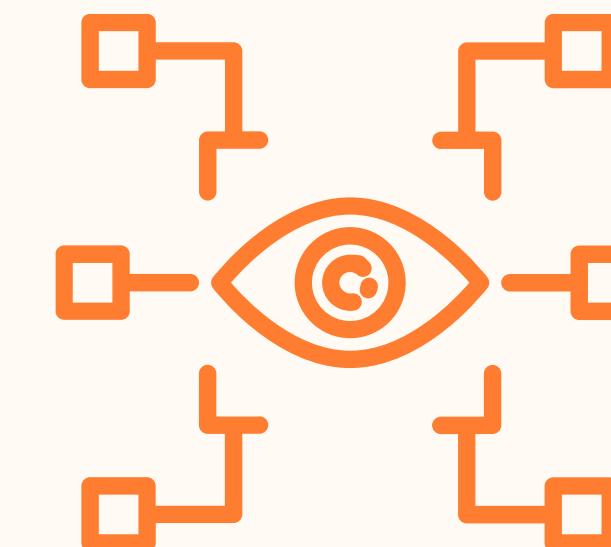
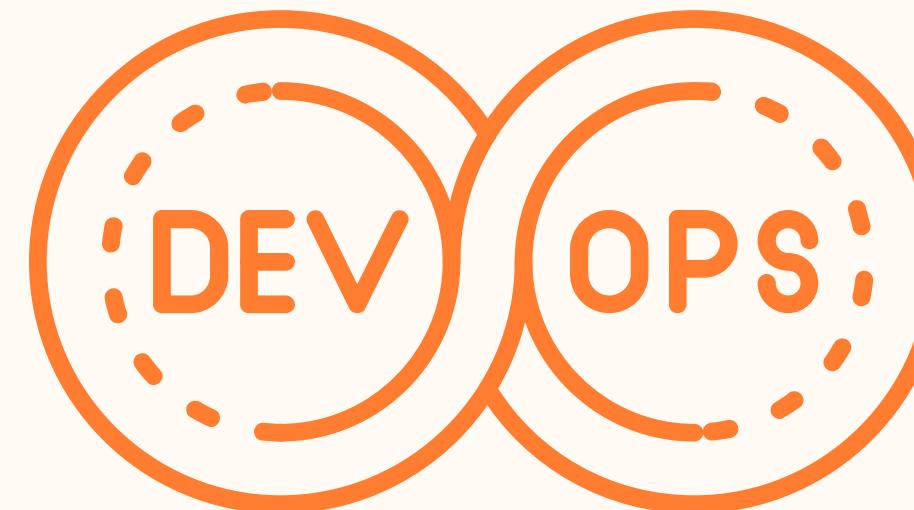


- MODÈLE DE RESPONSABILITÉ PARTAGÉE
- PRINCIPAUX ENJEUX





6. APPROCHE PROACTIVE





45 MIN

ANALYSE EN GROUPE

CAS PRATIQUE 1



SCÉNARIO

UNE ENTREPRISE A MIGRÉ UNE PARTIE DE SON SI VERS AZURE (CRM + ERP). ELLE CONSERVE UN DATACENTER INTERNE (HYBRIDE).

- UN BUCKET DE STOCKAGE CONTIENT DES DONNÉES INTERNES SENSIBLES.

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- IDENTIFIER LES RISQUES CONCRETS LIÉS À CETTE APPLICATION.
- ÉVALUER LEUR CRITICITÉ
- PROPOSER UNE MESURE DE PRÉVENTION
- PROPOSER UNE MESURE DE DÉTECTION
- DÉCRIRE UNE RÉPONSE EN CAS DE FUITE CONFIRMÉE.

RESTITUTION SUR FEUILLE / MAIL : esn@vidalfages.fr



CAS PRATIQUE 1



► Identification des risques concrets :

Catégories	Risques	Description
Confidentialité	Fuite de données depuis le bucket	Mauvaise configuration des permissions (accès public, clé partagée, compte compromis)
Intégrité	Altération ou suppression de données sensibles	Mauvais contrôle d'accès, absence de versioning, ransomware Cloud
Disponibilité	Indisponibilité du service CRM/ERP hébergé sur Azure	Dépendance réseau entre le site local et Azure (panne VPN, latence, erreur DNS)
Conformité / RGPD	Stockage de données personnelles hors UE ou sans clause contractuelle adaptée	Non-respect des exigences de localisation et de sous-traitance
Shadow IT / Gouvernance	Utilisation non maîtrisée de comptes Azure ou buckets personnels	Absence de gouvernance et de politique Cloud
Authentification / IAM	Compromission d'un compte administrateur Azure	MFA absent, mots de passe faibles ou partagés
Réseau hybride	Tunnel VPN ou ExpressRoute mal configuré	Fuite de trafic ou interception possible entre les environnements
Sauvegarde / Restauration	Absence de sauvegarde régulière des données du bucket	Perte définitive de données en cas de corruption ou suppression



CAS PRATIQUE 1

► Évaluation de la criticité :



		Impact		
		Important	Moyen	Faible
Probabilité	Important	Fuite de données sensibles (bucket)		Shadow IT
	Moyen	Compromission de compte Azure Admin	Altération de données / ransomware Absence de sauvegarde Cloud	
	Faible	Indisponibilité CRM/ERP (réseau ou panne Azure) Non-conformité RGPD		



CAS PRATIQUE 1

Mesures de prévention



Risque	Mesure de prévention
Fuite de données	Chiffrement au repos (SSE-KMS) et en transit (TLS) ; configuration des ACL strictes sur le bucket (principe du moindre privilège).
Compromission de compte	Activation du MFA sur tous les comptes administrateurs ; gestion centralisée via Azure AD / Entra ID ; rotation des clés d'accès.
Indisponibilité	Mise en place d'un plan de continuité d'activité (PCA) et réplication géographique sur Azure.
Non-conformité RGPD	Vérification du lieu d'hébergement des données et des clauses contractuelles (DPA) ; documentation des traitements.
Altération / ransomware	Sauvegardes immuables (Object Lock / versioning) et contrôle d'accès basé sur rôle (RBAC) .
Shadow IT	Mise en place d'une gouvernance Cloud (Cloud Policy / Azure Blueprint) avec suivi des déploiements.
Absence de sauvegarde	Déploiement de sauvegardes automatiques (Azure Backup / Blob Snapshot) .



CAS PRATIQUE 1

► Mesures de détection



Objectif	Mesure de détection
Activité suspecte sur le bucket	Azure Defender for Storage / CloudTrail / Log Analytics : détection d'accès inhabituels ou IP suspectes
Compromission de comptes	Audit Azure AD et alertes sur connexions anormales
Altération de données	Activation du versioning + journalisation des accès
Fuite réseau	IDS/IPS sur la liaison VPN / ExpressRoute
Conformité	Rapports automatiques via Azure Compliance Manager / Security Center



Réponse

CAS PRATIQUE 1



Étape	Action	Objectif
Identification	Identifier la source de la fuite (compte compromis, bucket public, clé exposée) via les logs Azure	Déterminer l'origine et la portée
Blocage	Révoquer les clés / tokens, isoler le bucket ou le compte compromis	Empêcher la propagation
Restauration	Restaurer les données à partir des sauvegardes immuables	Revenir à un état sûr
Communication	Notifier les utilisateurs et la CNIL (sous 72h si RGPD concerné)	Respect de la conformité
Analyse post-incident	Réaliser un rapport d'incident (type RCA – Root Cause Analysis) et renforcer les politiques IAM / logs / sécurité réseau	Prévenir la récurrence



45 MIN

ANALYSE DE GROUPE

SCÉNARIO

CAS PRATIQUE 2

“LA BASE DE DONNÉE ACCESSIBLE EN PUBLIQUE”



UNE START-UP UTILISE UNE BASE DE DONNÉE SAAS POUR SON SITE E-COMMERCE AVEC COMME DONNEES:

- IMAGES PRODUITS (NON SENSIBLES).
- LOGS CLIENTS (EMAILS, NUMÉROS DE CARTE PARTIELS).

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- IDENTIFIER LES RISQUES CONCRETS LIÉS À CETTE APPLICATION.
- ÉVALUER LEUR CRITICITÉ
- PROPOSER UNE MESURE DE PRÉVENTION
- PROPOSER UNE MESURE DE DÉTECTION
- DÉCRIRE UNE RÉPONSE EN CAS DE FUITE CONFIRMÉE.

RESTITUTION SUR FEUILLE / MAIL : esn@vidalfages.fr



CAS PRATIQUE 2

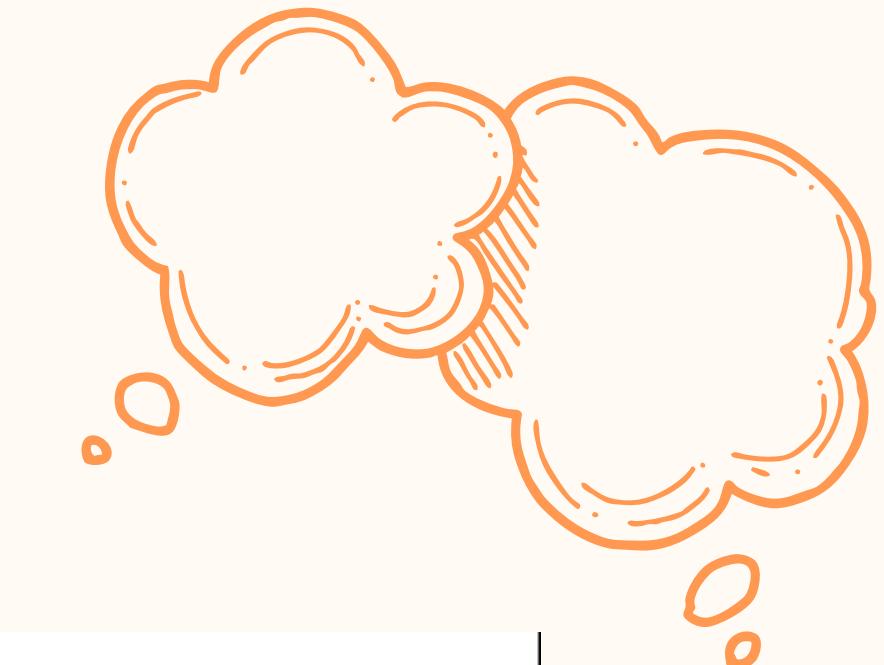
➤ Identification des risques concrets :



Catégorie	Risque concret	Description
Confidentialité	Fuite ou exposition des logs clients	Mauvaise configuration du stockage SaaS (bucket public, clé API exposée, partage externe non maîtrisé)
Intégrité	Altération ou suppression des logs	Mauvaise gestion des rôles / API ou injection SQL si interface exposée
Disponibilité	Indisponibilité de la base SaaS	Panne du fournisseur, attaque DDoS ou absence de plan de secours
Conformité / RGPD	Données personnelles exposées ou mal pseudonymisées	Logs contenant emails et fragments de CB = données personnelles
Authentification / IAM	Compromission du compte administrateur SaaS	Absence de MFA, mots de passe faibles, partage de compte
API / Exposition	Exploitation d'API publiques mal sécurisées	Endpoint non protégé ou trop permissif
Sauvegarde / Rétention	Perte de logs en cas d'incident ou purge automatique non maîtrisée	Pas de sauvegarde externe ou de rétention adaptée



CAS PRATIQUE 2

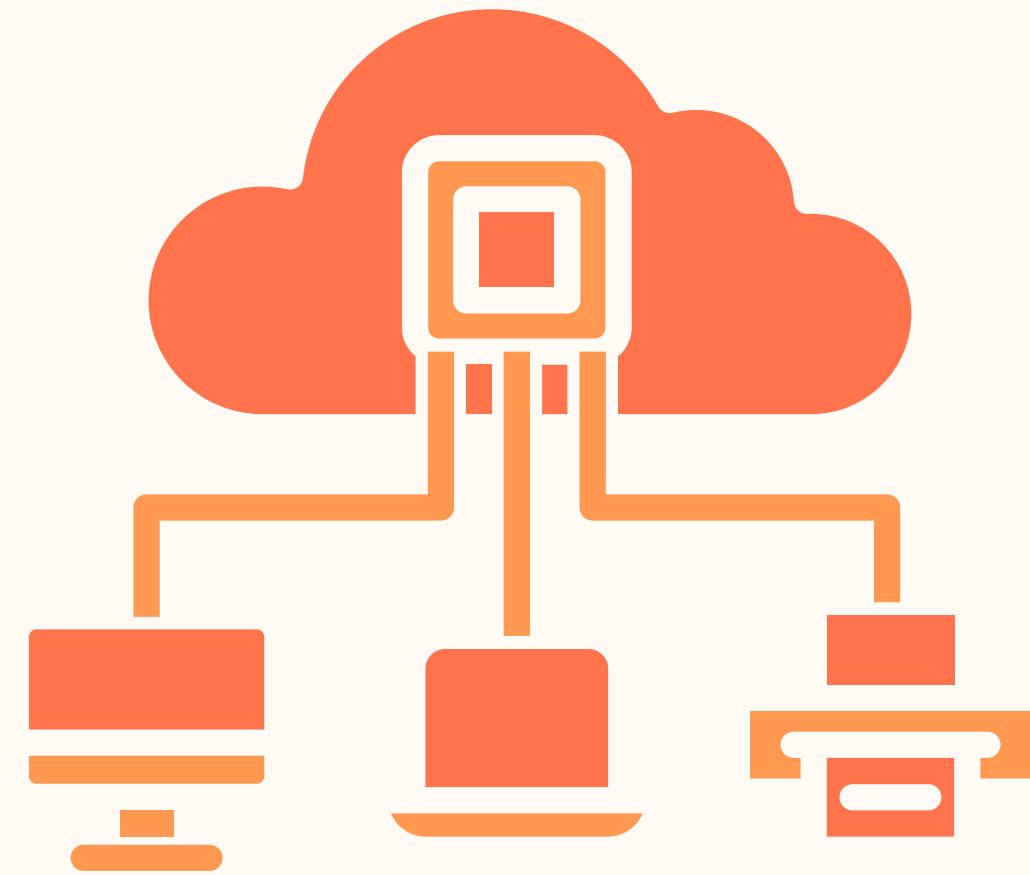


- Évaluation de la criticité :

		Impact		
		Important	Moyen	Faible
Probabilité	Important	Fuite des logs clients		Perte de logs
	Moyen	Compromission de compte Azure Admin - Non-conformité RGPD	Altération de données / ransomware Absence de sauvegarde Cloud	Perte ou vol d'image
	Faible	Indisponibilité du service		

CONCLUSION

- LA GESTION DES RISQUES CLOUD EST MULTIDIMENSIONNELLE (TECHNIQUE, ORGANISATIONNELLE, JURIDIQUE).
- PRÉVENTION, DÉTECTION ET CORRECTION DOIVENT ÊTRE INTÉGRÉES EN CONTINU.
- LA GOUVERNANCE ET LA CONFORMITÉ (RGPD, ISO, SECNUMCLOUD) SONT DES PILIERS INDISPENSABLES.



CHAPITRE 3 :

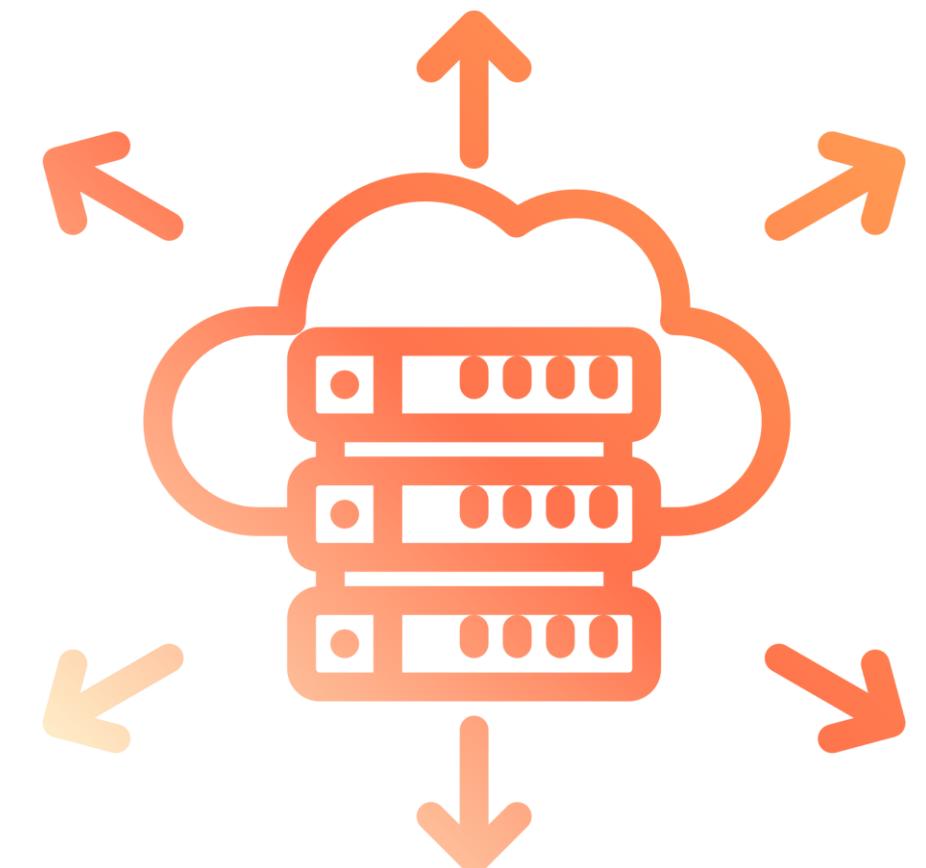
Stratégies de protection des données





Objectif

- **Confidentialité** : empêcher tout accès non autorisé (chiffrement, IAM)
- **Intégrité** : garantir que les données n'ont pas été altérées,
- **Disponibilité** : garantir l'accès aux données en cas d'incident,
- **Traçabilité** : assurer la journalisation et la détection d'anomalies





1. CONTEXTE ET ENJEU

2. CHIFFREMENT DES DONNÉES



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

- **Chiffrement au repos**
 - Données stockées sur disques, snapshots, bases de données, etc.
 - Objectif : protéger contre le vol physique ou la compromission d'un support.
 - Exemples : AWS S3 Server-Side Encryption (SSE-S3, SSE-KMS)
 Azure Storage Encryption



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

SSE-S3 (SERVER-SIDE ENCRYPTION – S3 MANAGED KEYS)

- Chiffrement géré entièrement par AWS S3.
- Les clés sont créées, stockées et gérées automatiquement par S3.
L'utilisateur n'a aucune action à faire pour la rotation ou la gestion des clés.
- Chiffrement réalisé avec AES-256.
Pas de journalisation fine des accès aux clés.
- Usage typique : pour les données standards sans exigence réglementaire forte.



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

SSE-KMS (SERVER-SIDE ENCRYPTION – AWS KEY MANAGEMENT SERVICE)

- Chiffrement géré par AWS KMS (Key Management Service).
Permet d'utiliser :
 - Soit une clé KMS par défaut gérée par AWS,
 - Soit une clé KMS personnalisée (CMK – Customer Managed Key).
- Offre un contrôle plus fin :
 - Droits IAM sur l'usage de la clé,
 - Journalisation CloudTrail de toutes les requêtes de chiffrement/déchiffrement,
 - Rotation automatique ou manuelle des clés.
- Usage typique : pour les environnements sensibles, réglementés ou audités (RGPD, ISO 27001...).



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

- **Chiffrement en transit**
 - Protection des flux entre client et serveur.
 - Outils : HTTPS, TLS 1.2+, SSH, VPN IPSec
 - **Cas typique** : communication entre une appli web et son backend API via HTTPS.



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

➤ Chiffrement applicatif

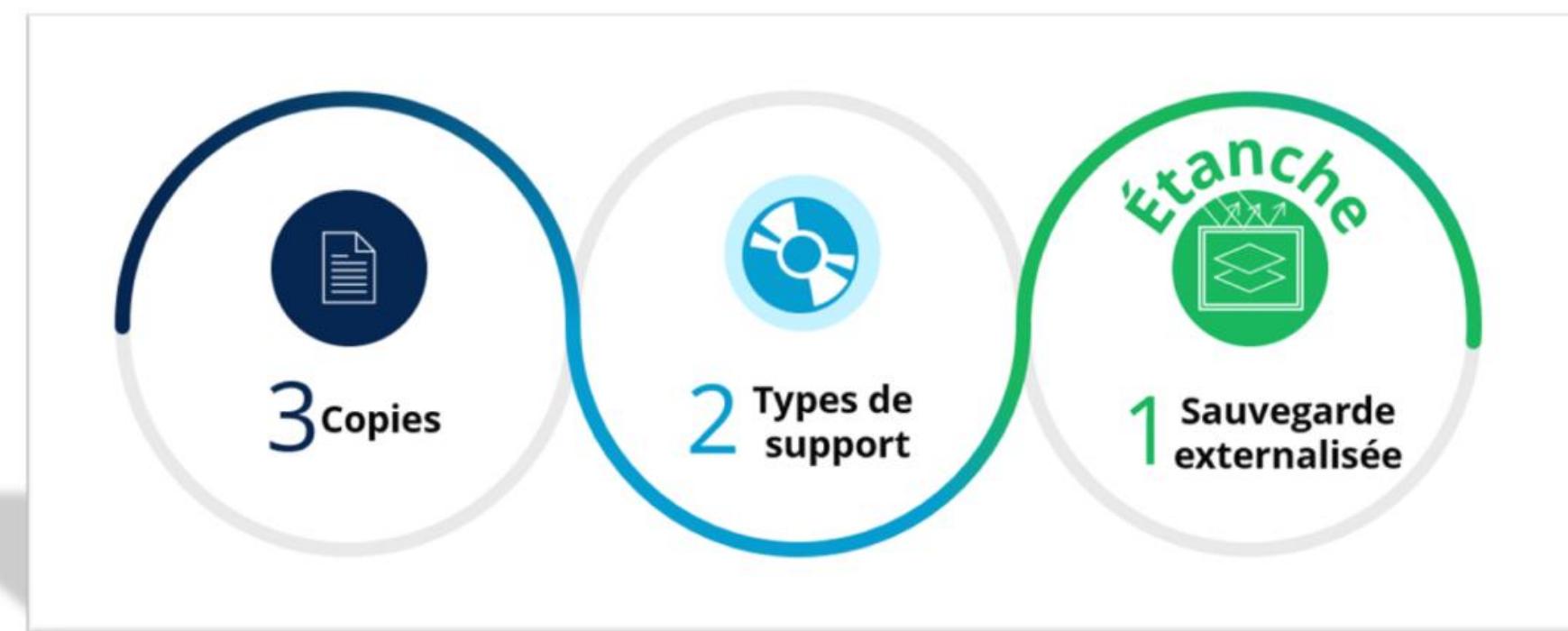
- Le chiffrement est géré directement par l'application.
- Exemple : les mots de passe utilisateurs stockés en hash (bcrypt, Argon2).
- Avantage : l'app reste sécurisée même si le stockage Cloud est compromis.

Question :

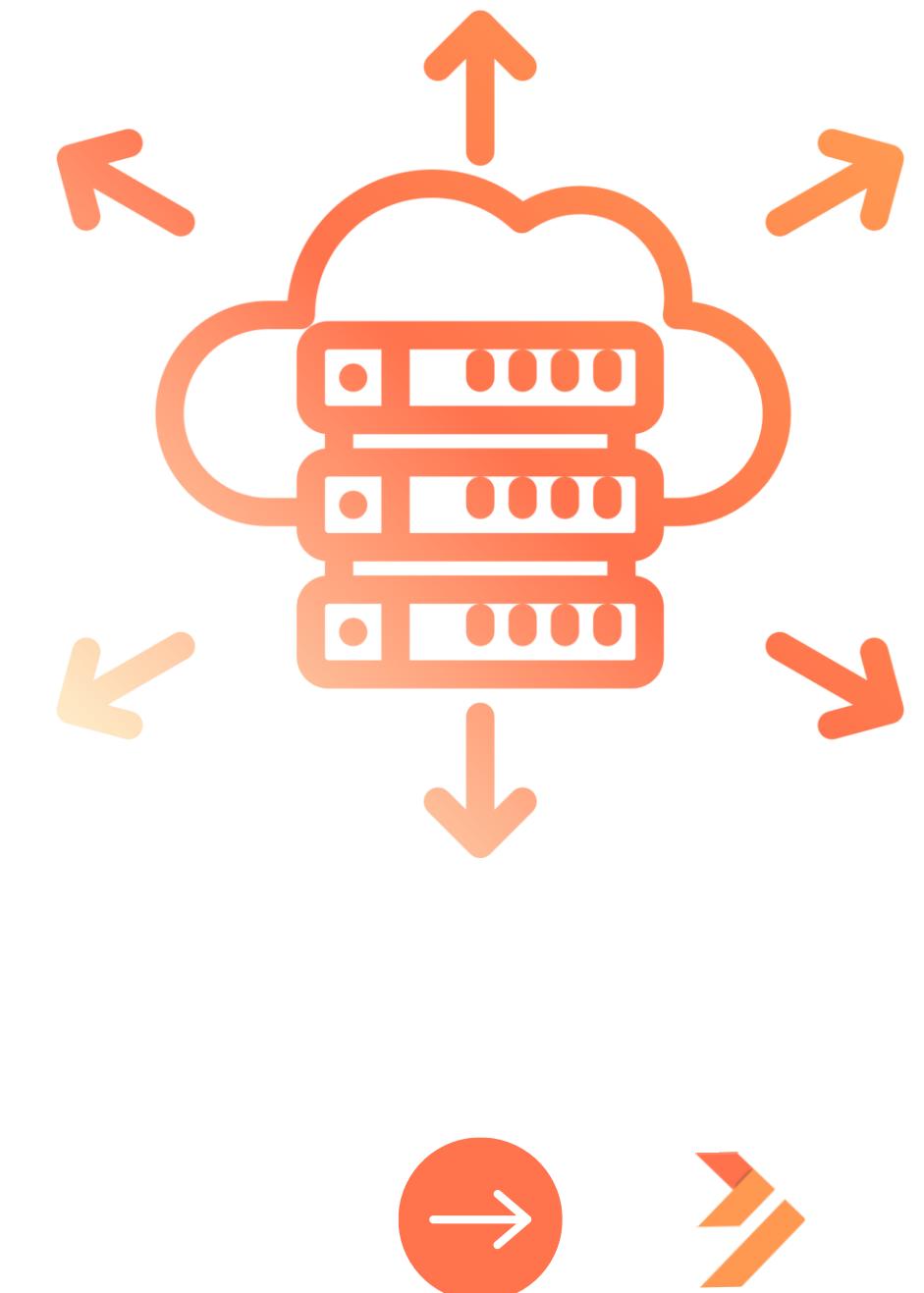
Pourquoi le chiffrement applicatif peut-il être préférable à un chiffrement natif Cloud ?

SAUVEGARDE ET RESTAURATION

- Objectif : garantir la continuité de service (BCP/DRP).
- Stratégies :
 - Sauvegarde complète, différentielle, incrémentale.
 - Rétention : définir le temps de conservation des sauvegardes.
 - Test de restauration obligatoire (ne jamais se fier à la sauvegarde seule).



Exemples : AWS Backup, Azure Recovery Services Vault, GCP Backup for GKE.



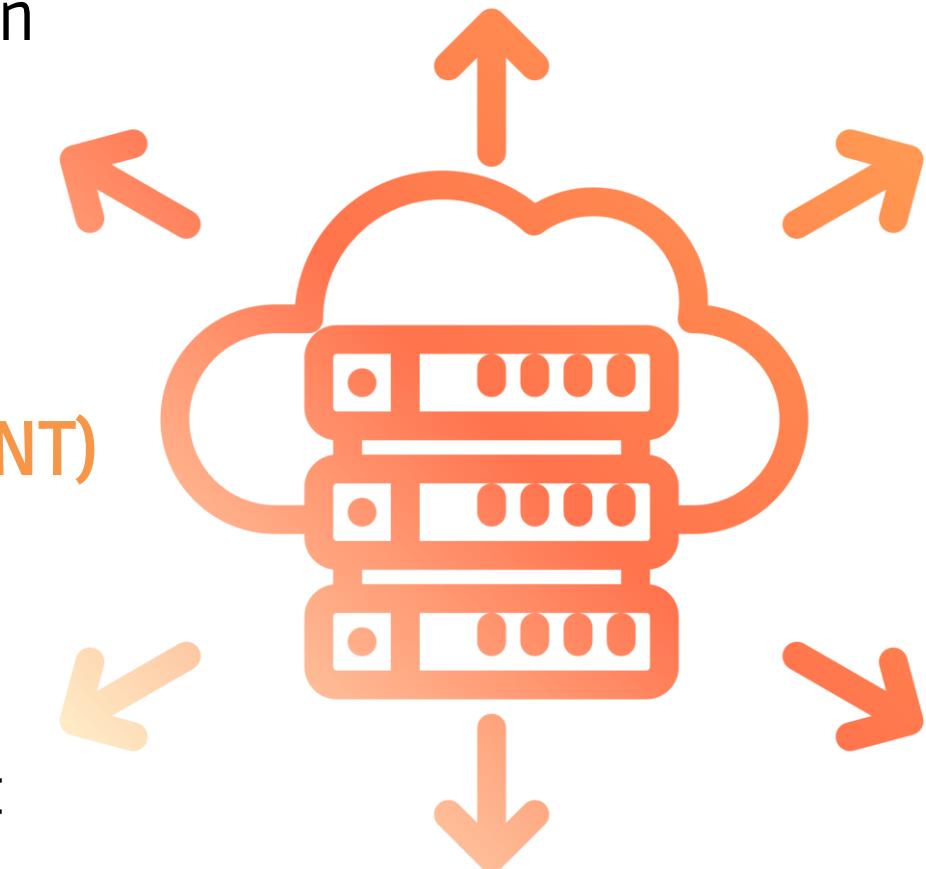
SAUVEGARDE ET RESTAURATION

➤ RTO – RECOVERY TIME OBJECTIVE (OBJECTIF DE TEMPS DE RÉTABLISSEMENT)

C'est le temps maximal acceptable pour restaurer un service ou une application après un incident.

Combien de temps maximum peut-on rester en panne avant que cela ait un impact critique sur l'activité ?

Si ton RTO est de 2 heures, cela signifie que ton système doit être opérationnel au plus tard 2 h après la panne.



➤ RPO – RECOVERY POINT OBJECTIVE (OBJECTIF DE POINT DE RÉTABLISSEMENT)

C'est la quantité maximale de données que l'on peut se permettre de perdre, exprimée en temps entre la dernière sauvegarde et la panne.

Quelle ancienneté maximale des données peut-on accepter après un incident ? Exemple : Si ton RPO est de 15 minutes, cela veut dire qu'en cas de panne, tu peux perdre au maximum 15 min de données.

Exemples : AWS Backup, Azure Recovery Services Vault, GCP Backup for GKE.



Gestion des accès et conformité

- **IAM (Identity & Access Management) :**
 - Politique du moindre privilège. (zero trust)
 - Groupes et rôles (plutôt qu'utilisateurs individuels).
- **Audit de conformité :**
 - RGPD (Europe), ISO 27018 (Cloud privacy), SOC 2 Type II (contrôles internes).
 - CloudTrail, Azure Monitor, GCP Audit Logs.
- **Journalisation et alerte :**
 - Détection d'anomalies (ex. : connexion depuis un pays inhabituel).



ACTIVITÉ PRATIQUE

SCÉNARIO



Une PME migre son serveur de fichiers local vers un espace de stockage AWS (S3 Bucket) et une base de donnée AWS (RDS).

Elle stocke des données clients et RH sensibles.

- Identifier les risques.
- Proposer une stratégie complète : chiffrement, clés, sauvegarde, IAM.