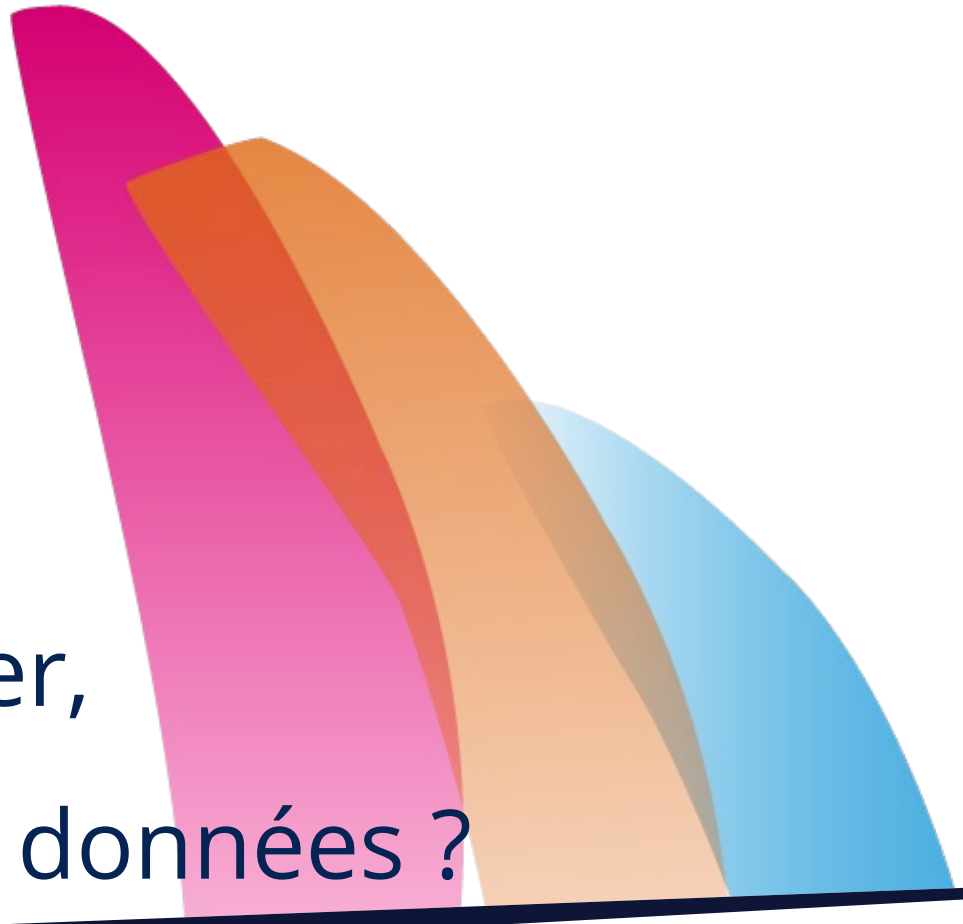

cci
NOUVELLE-CALÉDONIE

Rendez-vous de l'économie

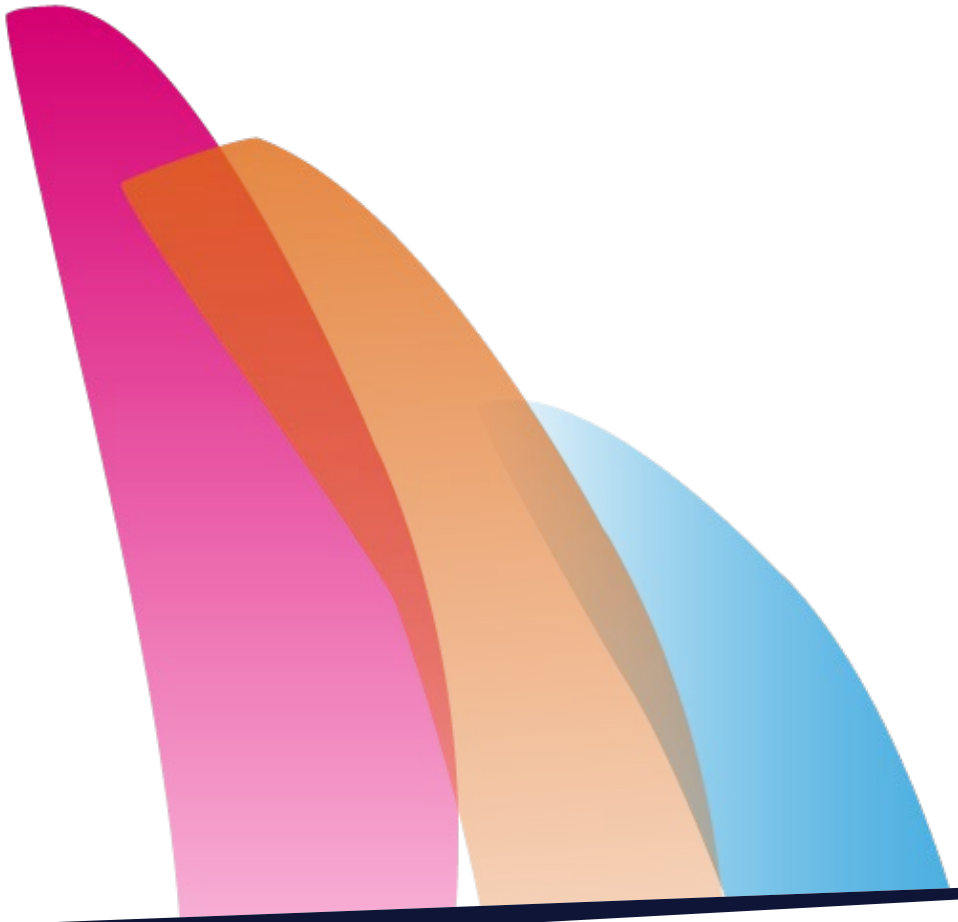
Entreprises, comment stocker, sauvegarder et protéger vos données ?



cci NOUVELLE-CALÉDONIE

La sécurité des données : définition et enjeux

Par Cédrick DEMENE



cci NOUVELLE-CALÉDONIE

Qu’est-ce qu’une donnée et comment la classifier ?

- une donnée est la représentation d’une information dans un programme. Cela peut être sous forme de texte dans le code source ou en mémoire pendant l’exécution du programme. Les données peuvent être de différents types : textuelles, numériques, images, sons, etc

- La classification des données est essentielle pour organiser et protéger les informations en fonction de leur sensibilité et de leur importance.

Qu’est-ce que la sécurité des données ?

La notion de sécurité des données regroupe l’ensemble des moyens employés pour protéger les informations numériques contre les accès non autorisés, les compromissions et les vols, tout au long de leur cycle de vie.

Avec un triple objectif :

- Garantir la confidentialité
- Garantir l’intégrité
- Garantir la disponibilité des données de l’entreprise

Pourquoi la sécurité des données est-elle cruciale ?

- Un environnement informatique fragmenté et des risques élevés
- Des utilisateurs plus attentifs à la protection des données personnelles
- Protection des données : des risques financiers à ne pas négliger

Comment assurer la sécurité des données informatiques ?

Pour assurer la sécurité des données numériques, les entreprises doivent s'appuyer sur ces piliers :

•Le choix d'une infrastructure cloud sécurisée pour ses données sensibles (cloud privé, cloud qualifiés …)

•L'implémentation d'outils de collaboration sécurisés (des solutions secure by design, des logiciels de confiance, certifiés et/ou qualifiés pour un environnement de travail protégé)

•une gestion optimisée des cybermenaces (outils de détection, protocole de gestion de crise, plan de reprise ou de continuité d'activité)

Quelles sont les bonnes pratiques pour la sécurité des données ?

•Une identification des données sensibles de son organisation et la mise en place d'un système de classification interne

•La mise à jour des applications, logiciels et systèmes d'exploitation de l'entreprise, afin qu'ils intègrent en permanence les derniers correctifs de sécurité.

•L'utilisation de technologies qui renforcent la sécurité des données : antivirus, pare-feu, VPN, etc.

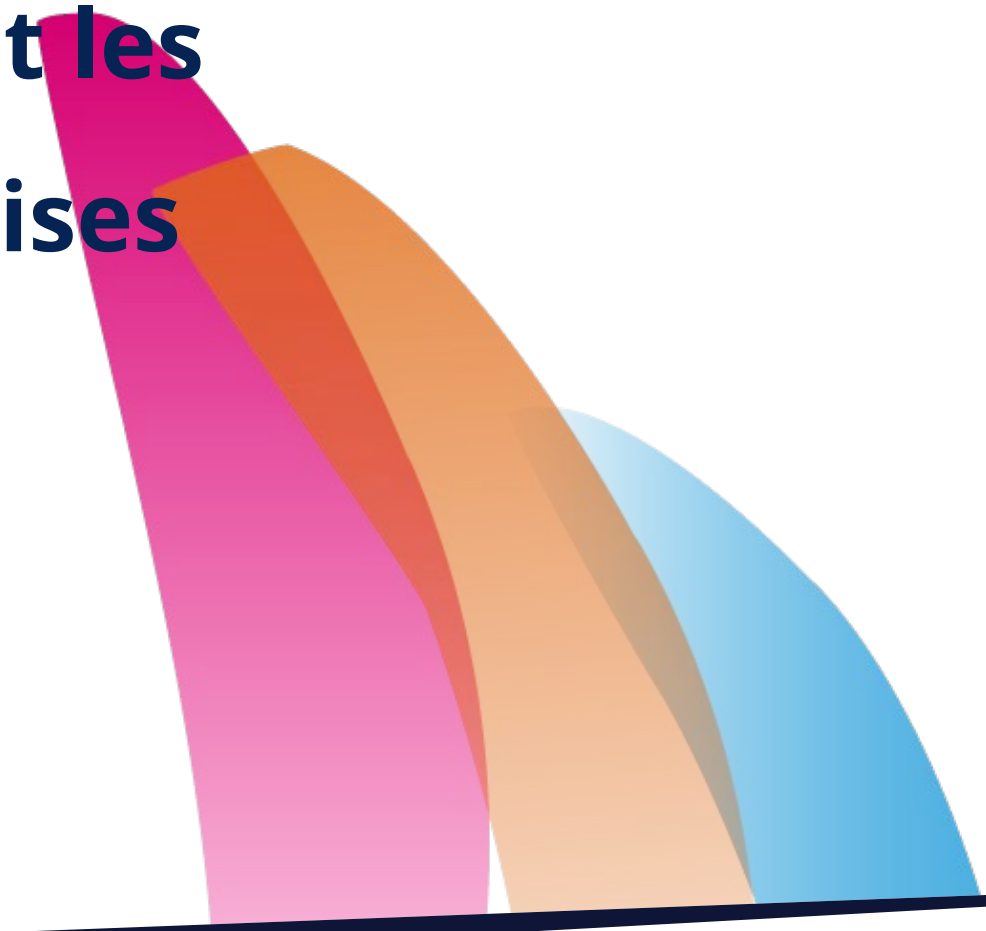
•La gestion des accès aux systèmes d'information et aux outils collaboratifs.

•La sensibilisation des collaborateurs à la sécurité des données et à ses enjeux, Quelques exemples : changer régulièrement de mot de passe, ne pas ouvrir d'e-mail suspect ni cliquer sur des liens inconnus, bannir les sites non sécurisés, ne jamais divulguer d'informations sensibles par voie électronique (même si la demande émane d'un supérieur hiérarchique), etc.

•La réalisation de sauvegardes régulières des données sensibles et stratégiques, afin de pouvoir les restaurer au plus vite en cas de sinistre ou d'attaque.

Le stockage de données et les solutions pour les entreprises

Par Jocelyn TANGUY



cci NOUVELLE-CALÉDONIE

Entreprises, comment stocker, sauvegarder et protéger vos données ?

Jocelyn TANGUY

Responsable commercial chez DSP – Data Services Pacific

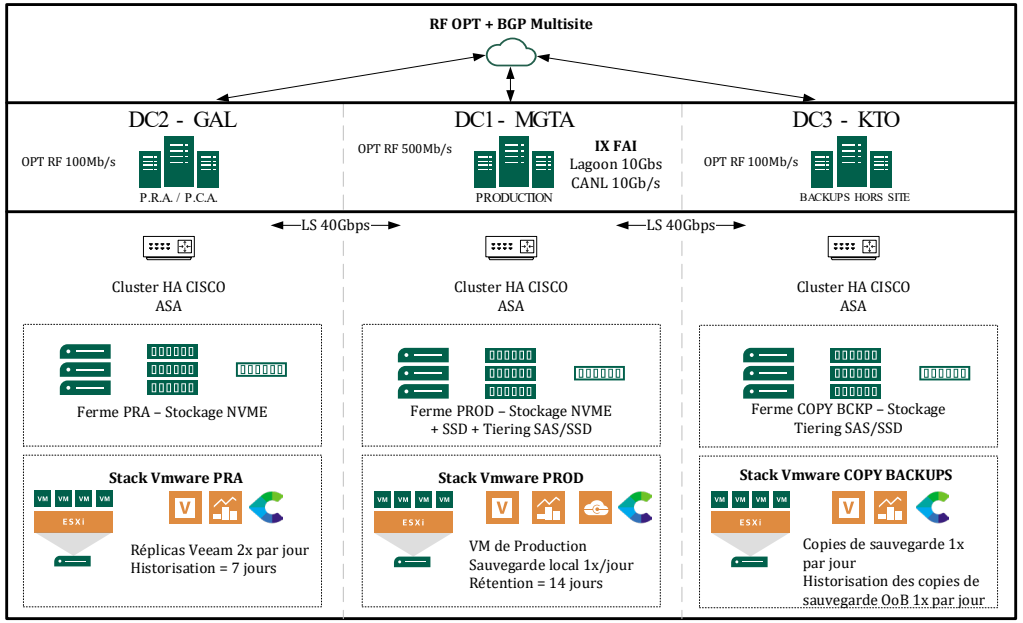
Tel : +687 754.704

Email : j.tanguy@dsp.nc

3ème vice-président du cluster OPEN NC

Qui sommes-nous ?

- ✓ **Création : 2011,**
- ✓ **2 Datacenters en propre** + interconnexion sur 3ème Datacenter,
- ✓ **Pure player** avec une activité 100% dédiée datacenter,
- ✓ **+ 120 clients** en Nouvelle-Calédonie,



- ✓ **Support 24 heures sur 24 – 7 jours sur 7 (N1+N2),**
- ✓ Ecosystème riche (**FAI / IXP/ IX SANTE**),
- ✓ **Connectivité** → 3 FAIs + RF OPT – Redondance des liens physiques,
- ✓ **SLA à partir de 99,8%.**

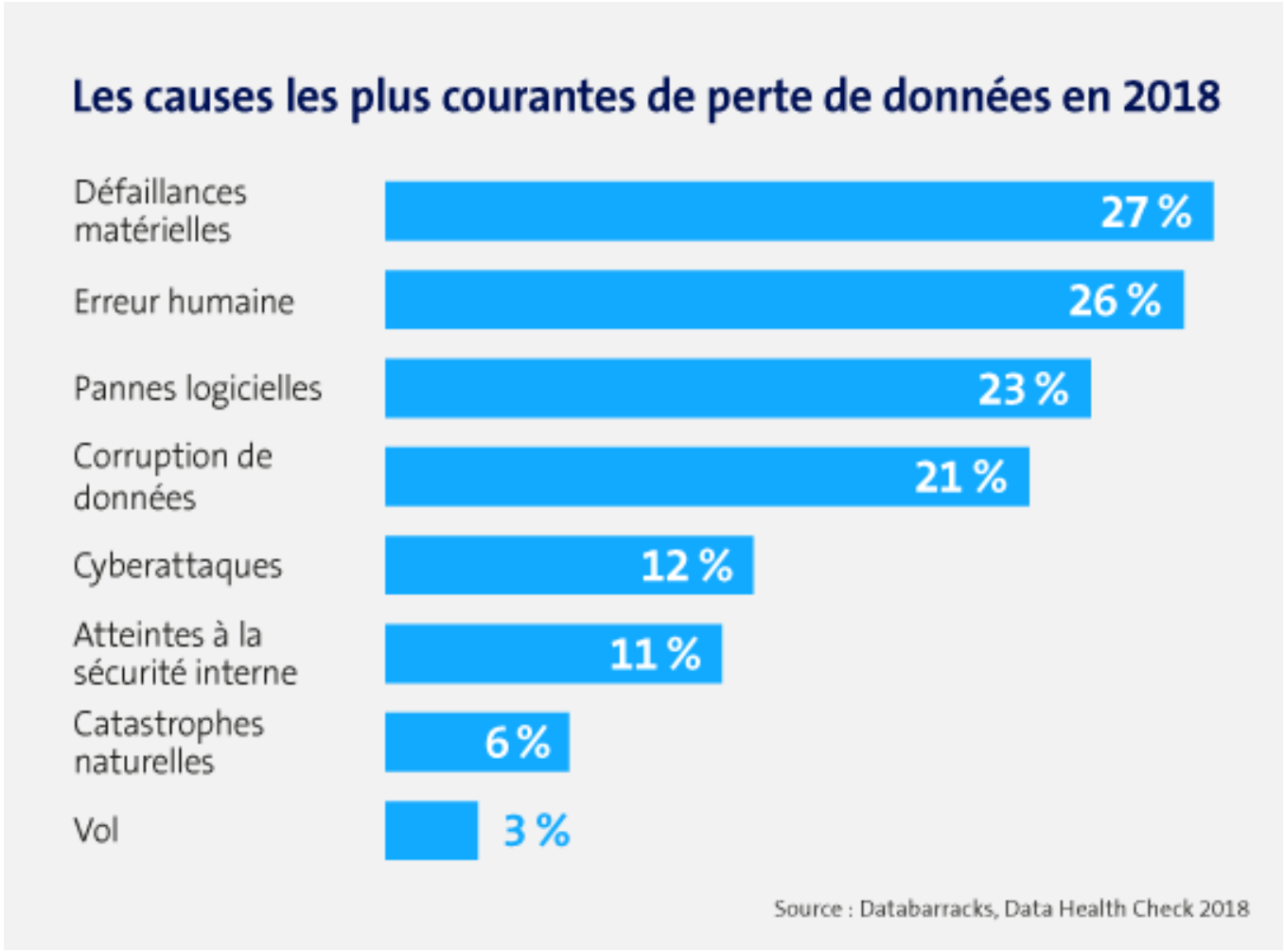
Collocation de racks

Infrastructure

Sauvegarde

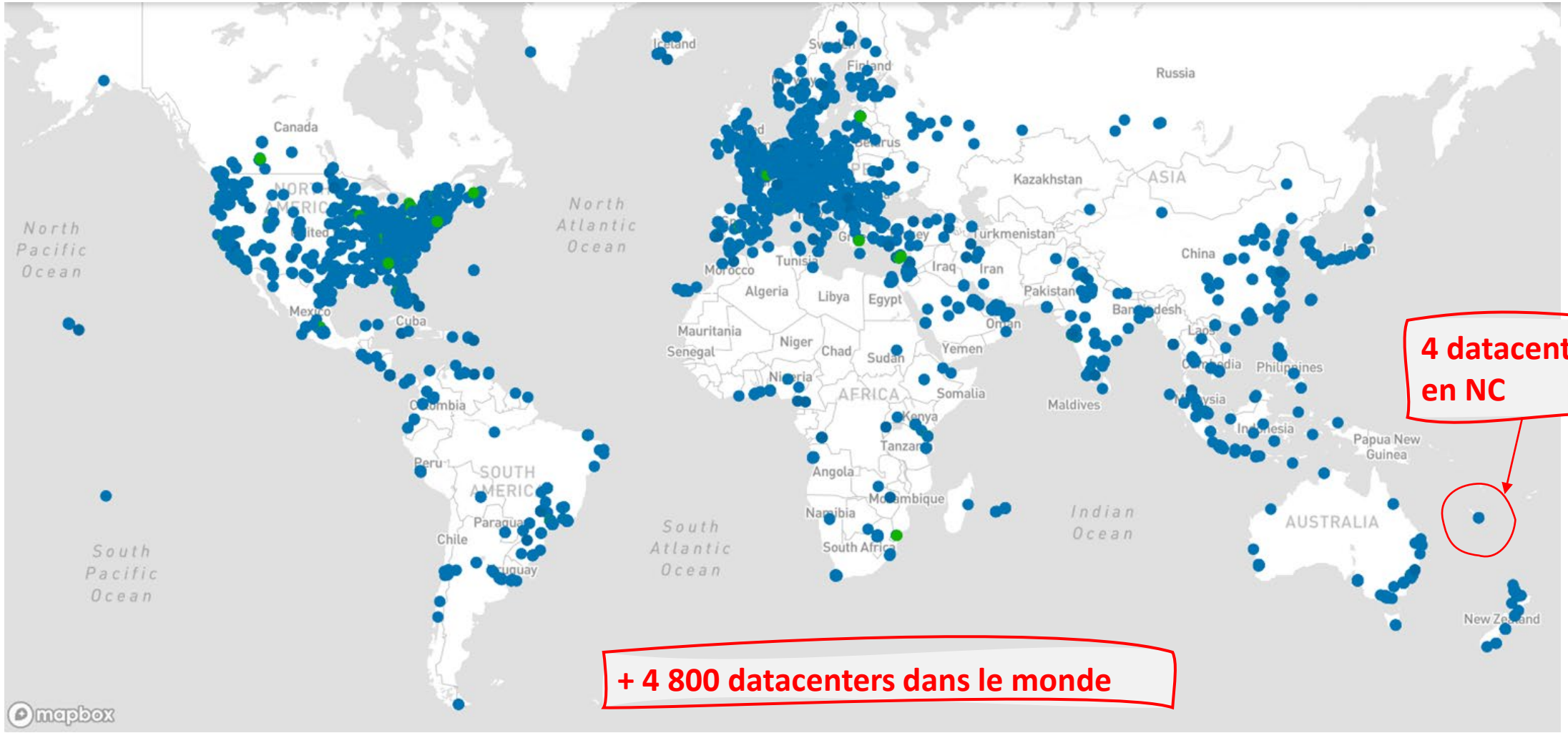
Plan de Reprise d'Activité

Rappel - Les causes de pertes de données

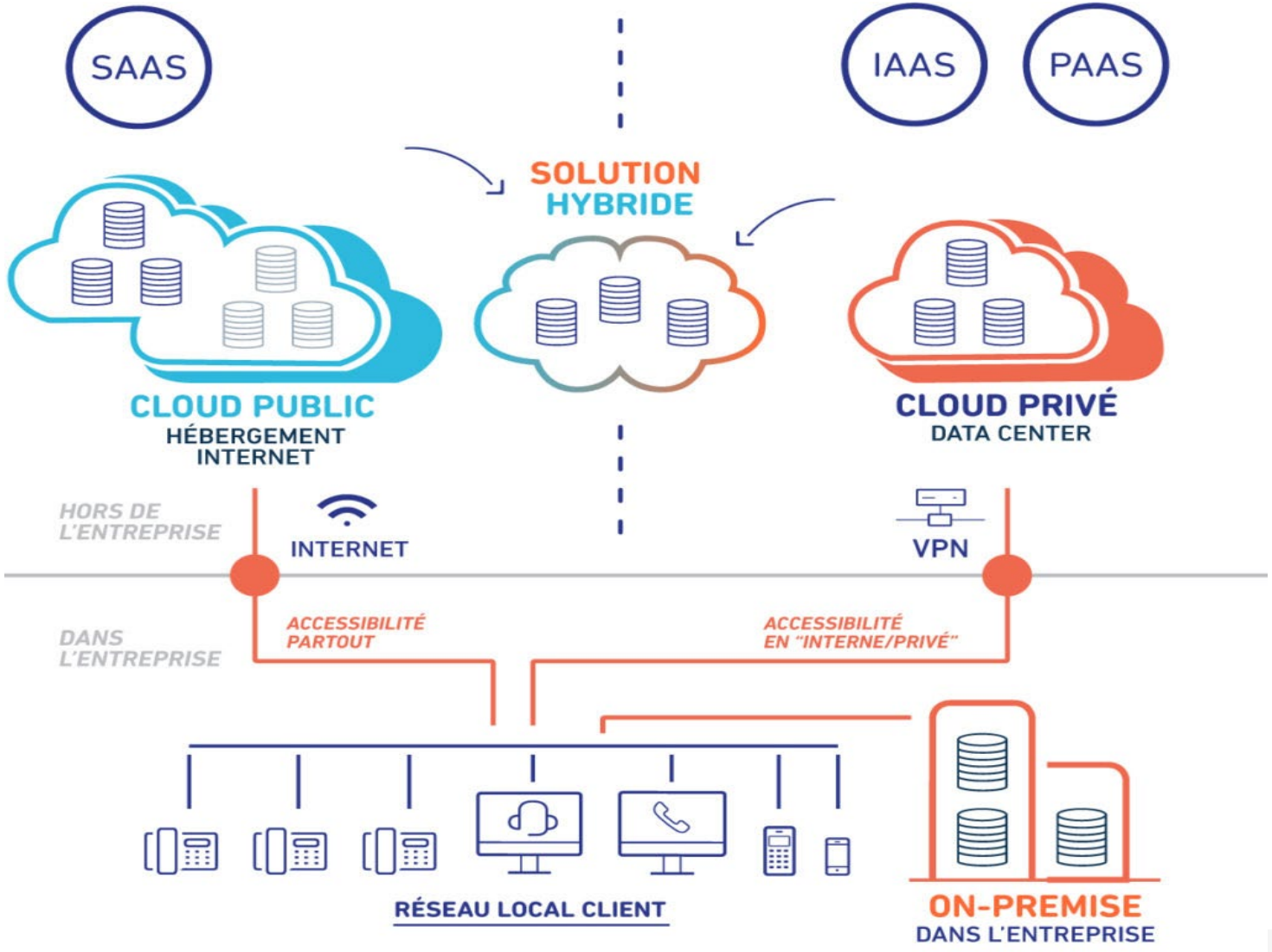


La question n'est pas « SI » mais « QUAND » ?

Le cloud, une multitude de datacenters



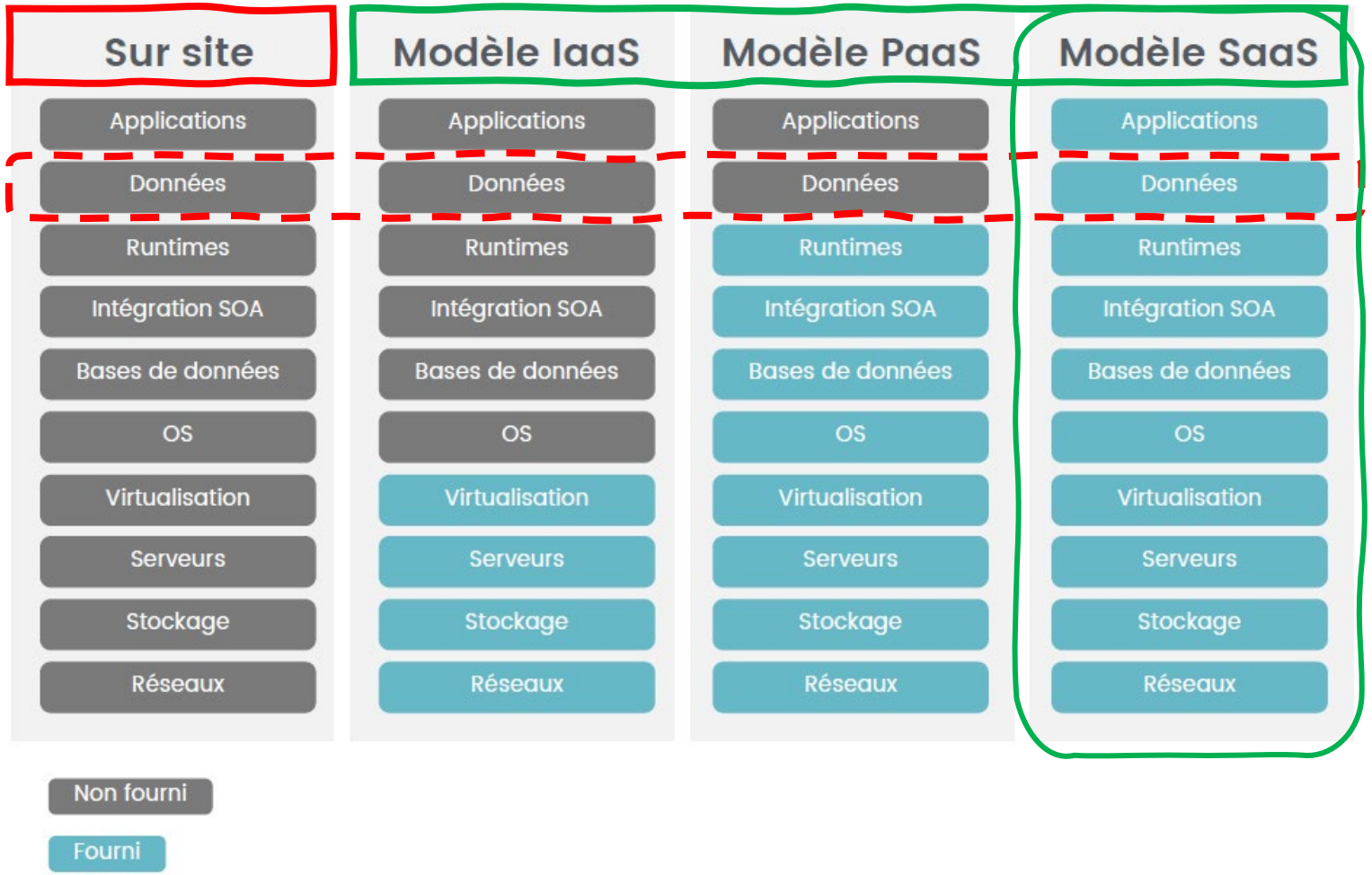
3 types de Cloud, une multitude de solutions



Les typologies de Cloud

Cloud Public	Cloud Privé	Cloud Hybride	
Aucun Cout de Maintenance	Dédié et Sécurisé	Politique de déploiement piloté	PLUS
Flexibilité	Conformité Réglementaires	Flexibilité	
Simplicité	Sur Mesure	Gestion centralisée de la sécurité	
Investissement minimal	Evolutivité	Ressources diverses et évolutivité rapide	
Agilité et Innovation	Gestion Complète	Capacité de débordement rapide	
Certifications réglementaires variées	Proximité	Panel Technologique	
Risque TCO important	TCO Maîtrisé	TCO Important	MOINS
Contrôle Minimal	Compétence technique nécessaire	Compétence technique nécessaire	

Quelles solutions sont possibles ?



Hébergement

=

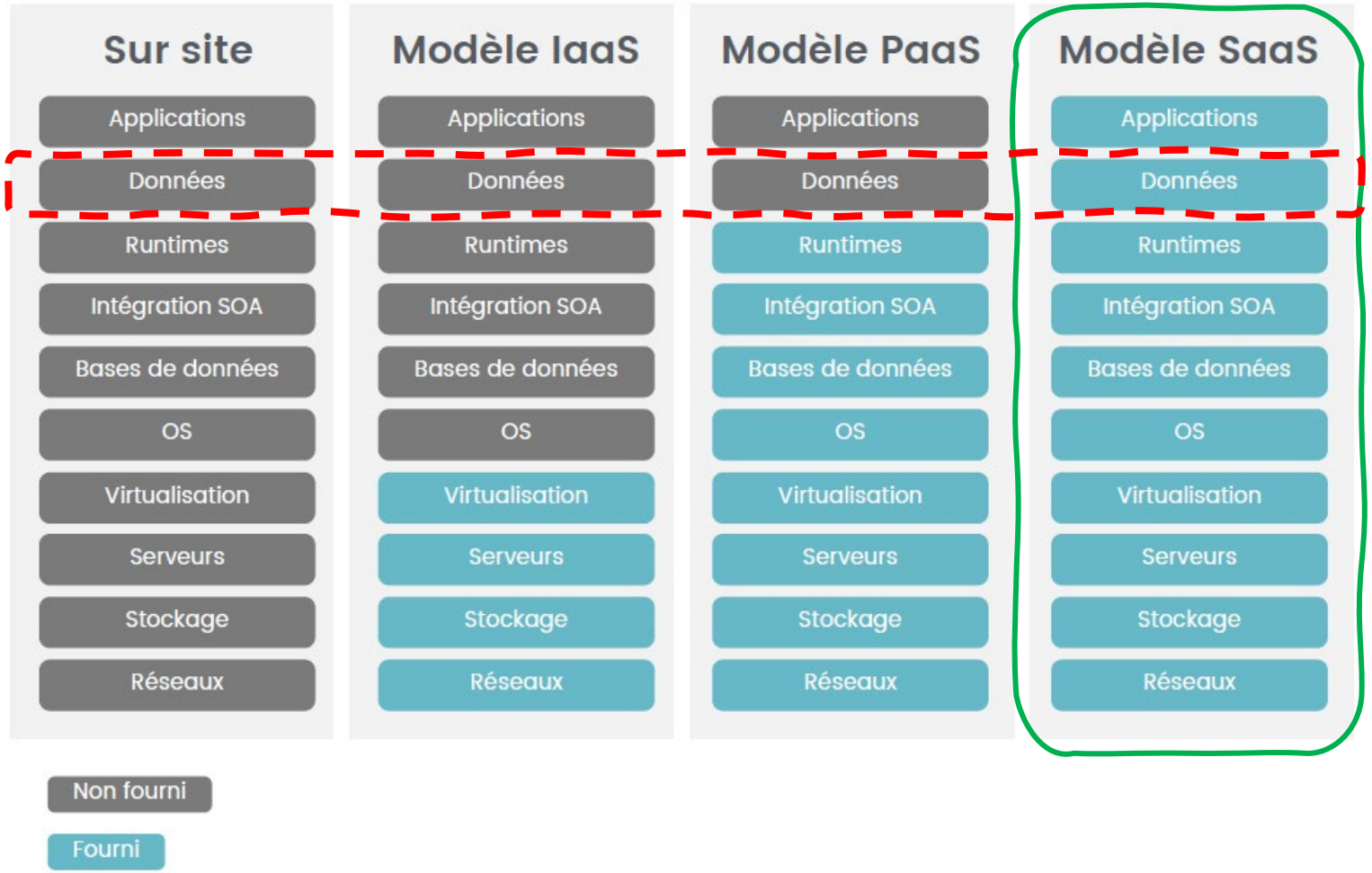
Granularité de la gouvernance.

Les données:

- Votre responsabilité
- Votre priorité

SaaS – Software as a Service

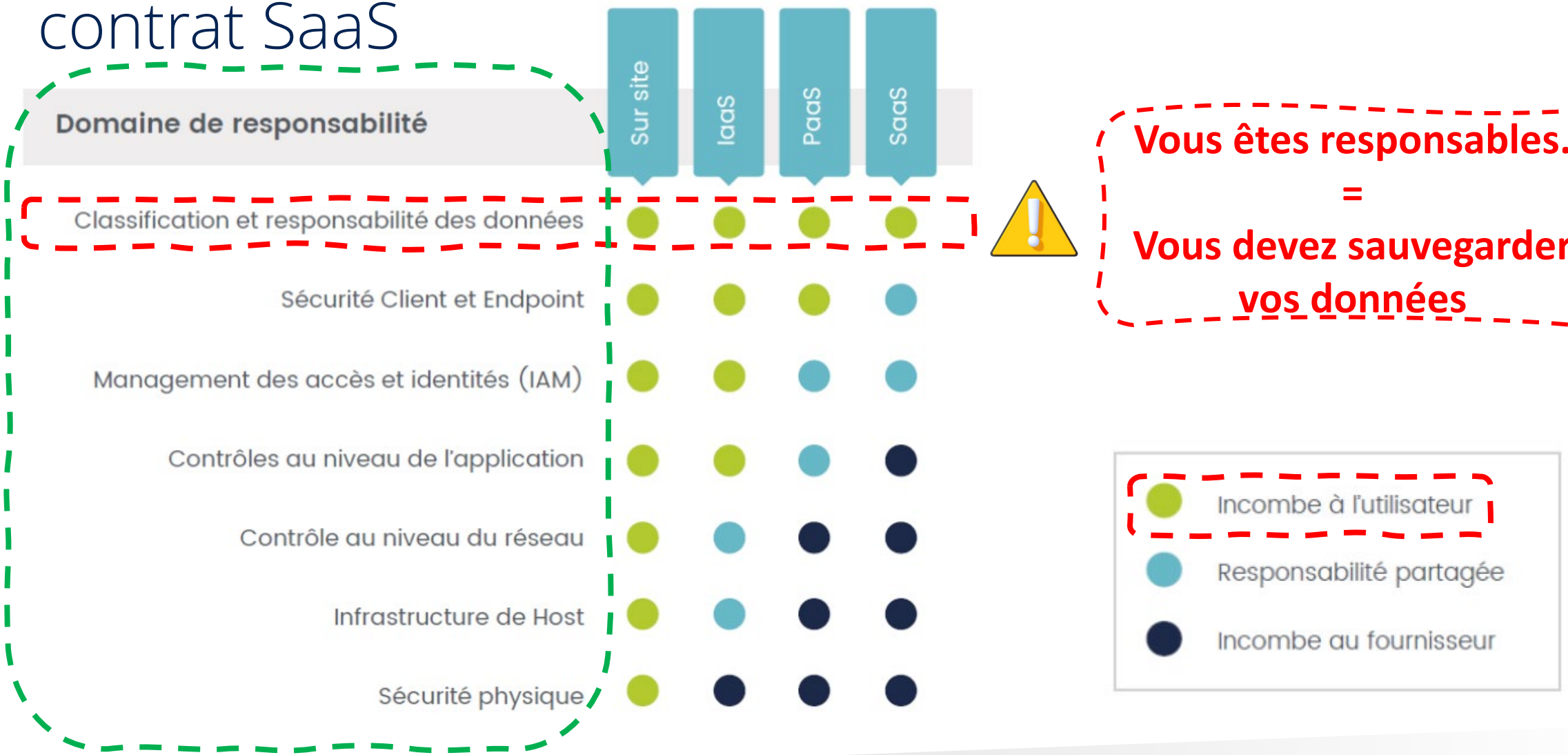
SaaS – Software as a Service



Le prestataire garantit la disponibilité des données.

cci NOUVELLE-CALÉDONIE

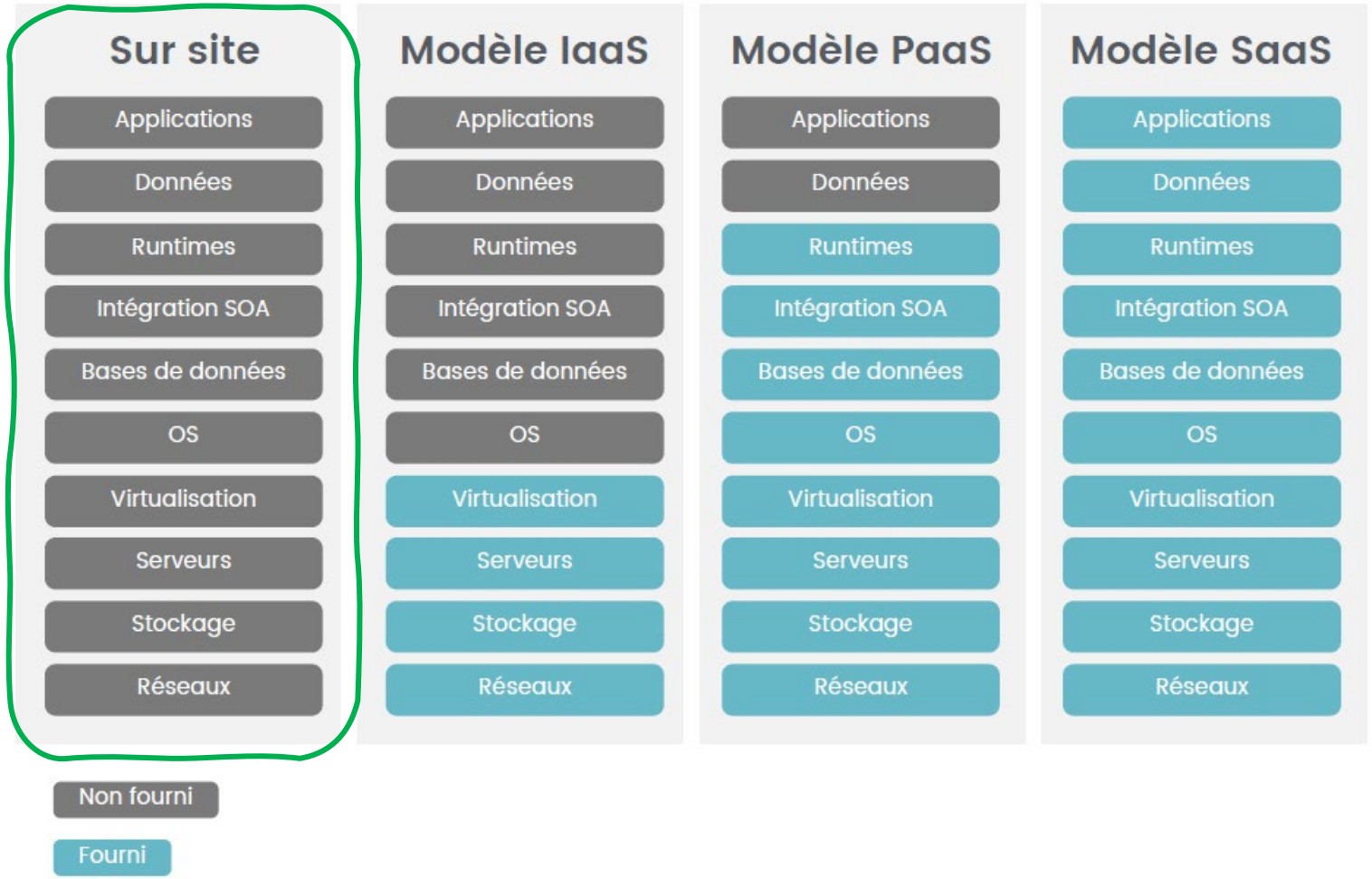
SaaS – Les points à vérifier avant de signer un contrat SaaS



Sur Site – Objectif sauvegarde

Vous êtes responsables de TOUT.

Mettre en place les outils et une stratégie de sauvegarde est votre priorité.



La Sauvegarde : Les bases

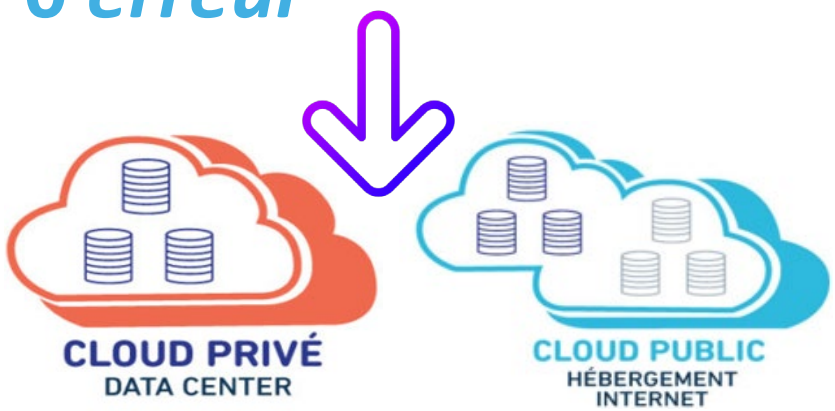
3 copies différentes

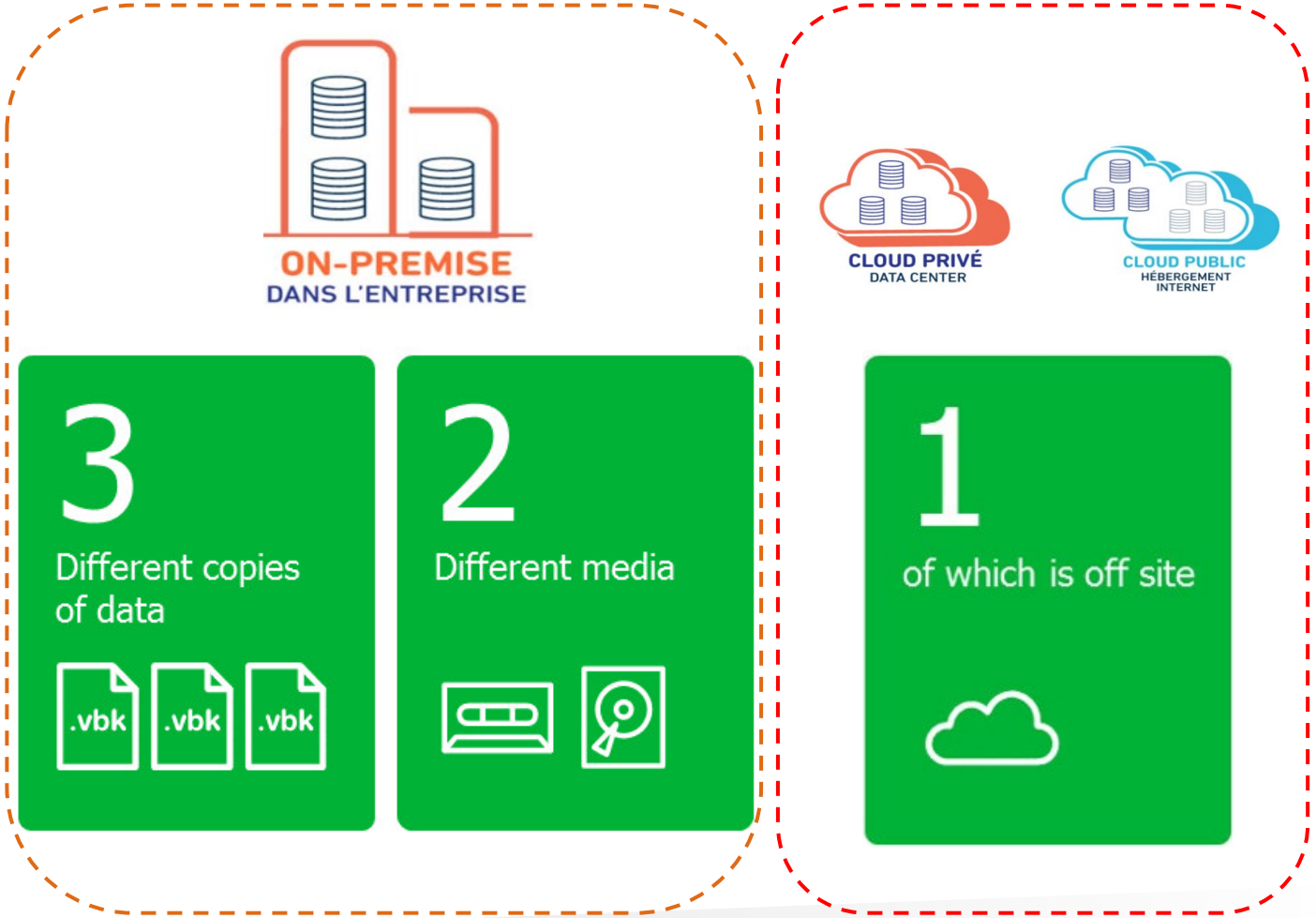
2 supports différents

1 copie hors site

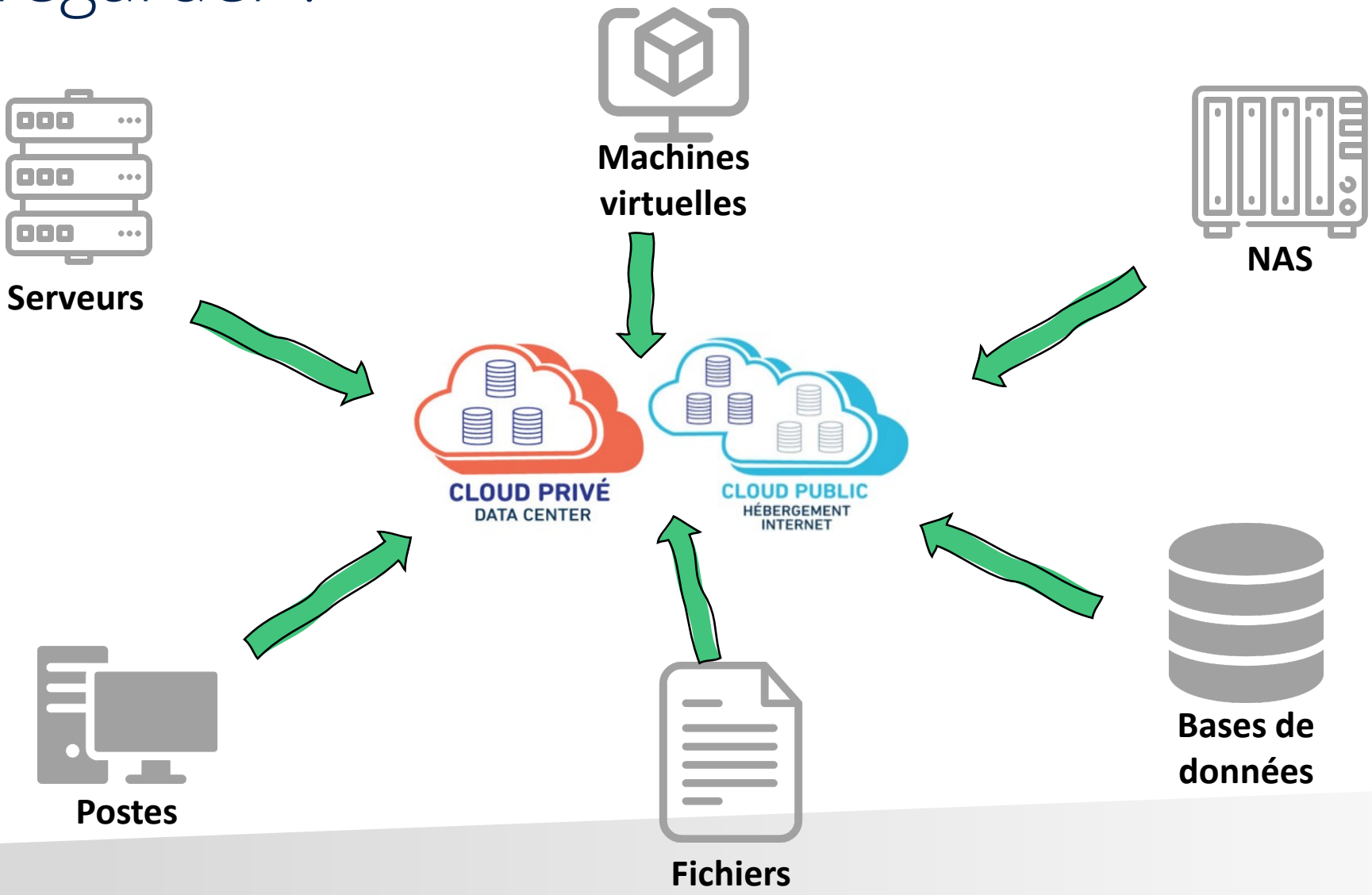
1 copie hors ligne

0 erreur

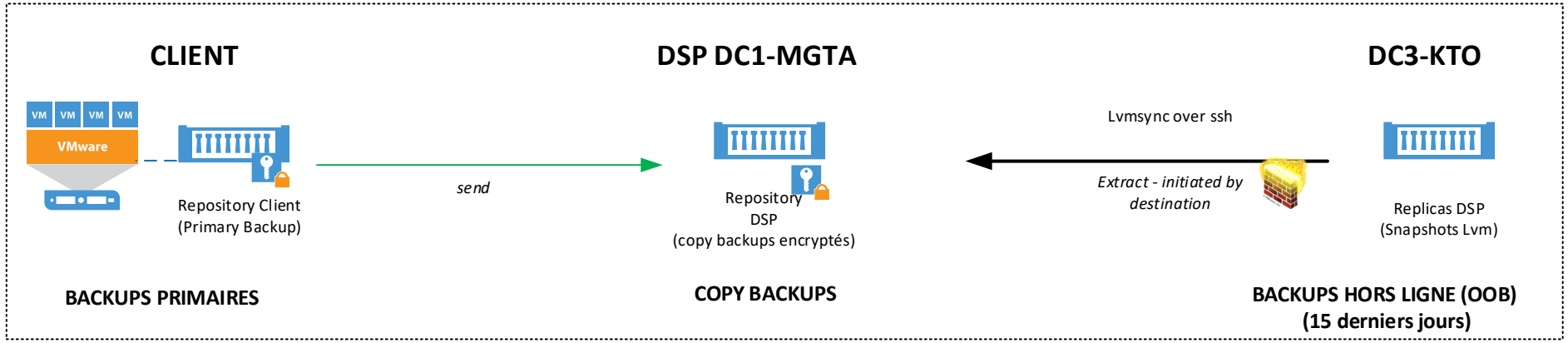




Sauvegarde vers le Cloud : Que peut-on sauvegarder ?



BaaS - La Sauvegarde en tant que service.



Prestataire d'infogérance de sauvegarde prend en charge:

- Logiciel de sauvegarde
- Configuration
- Surveillance
- Externalisation des données
- Restauration à la demande
- Accompagnement
- Surveillance et suivi
- Conseil

La Sauvegarde – Les bonnes pratiques

- **Définir la stratégie de rétention appropriée aux risques que vous voulez mitiger**
- **Sauvegarder régulièrement**
- **Plusieurs supports**
- **Plusieurs sites**
- **Vérifier et tester régulièrement**
- **Une infrastructure de sauvegarde décorrélée de l'environnement de production**

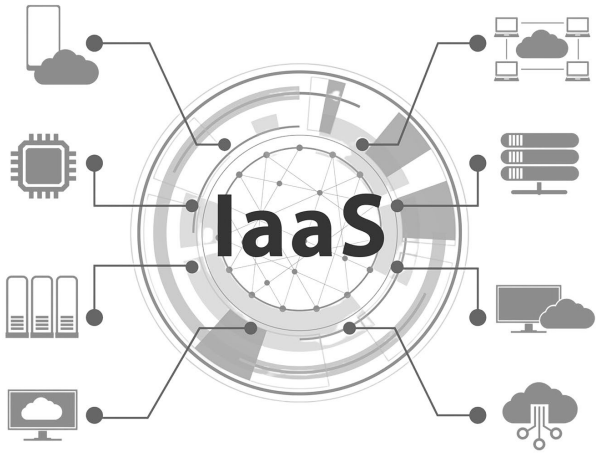
IaaS – Infrastructure as a Service

Sur site	Modèle IaaS	Modèle PaaS	Modèle SaaS
Applications	Applications	Applications	Applications
Données	Données	Données	Données
Runtimes	Runtimes	Runtimes	Runtimes
Intégration SOA	Intégration SOA	Intégration SOA	Intégration SOA
Bases de données	Bases de données	Bases de données	Bases de données
OS	OS	OS	OS
Virtualisation	Virtualisation	Virtualisation	Virtualisation
Serveurs	Serveurs	Serveurs	Serveurs
Stockage	Stockage	Stockage	Stockage
Réseaux	Réseaux	Réseaux	Réseaux

Non fourni

Fourni

Le prestataire garantit l'infrastructure
=
Mise à disposition de capacité de calcul, de mémoire et de stockage (CPU – RAM – HDD)

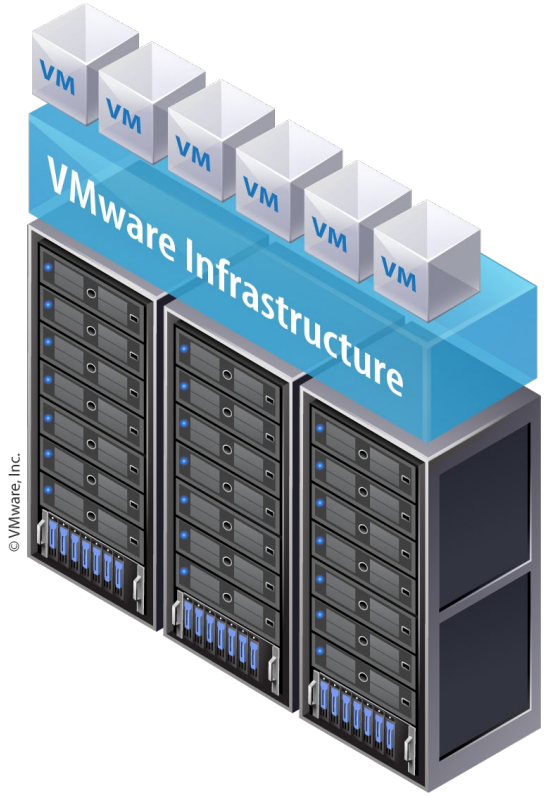


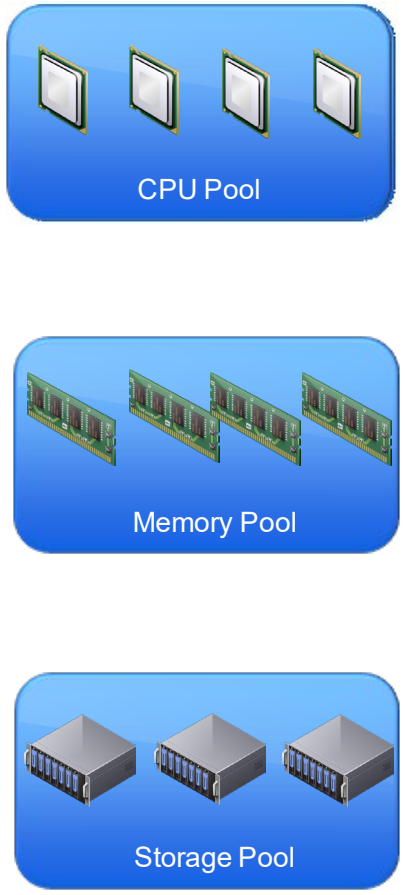
cci NOUVELLE-CALÉDONIE

IaaS – Infrastructure as a Service.

Une multitude de serveur dans un datacenter sécurisé :

- Processeurs
- Mémoire
- Stockage
- Un socle de virtualisation robuste
- Supervision
- Niveaux de service





IaaS – Infrastructure as a Service.

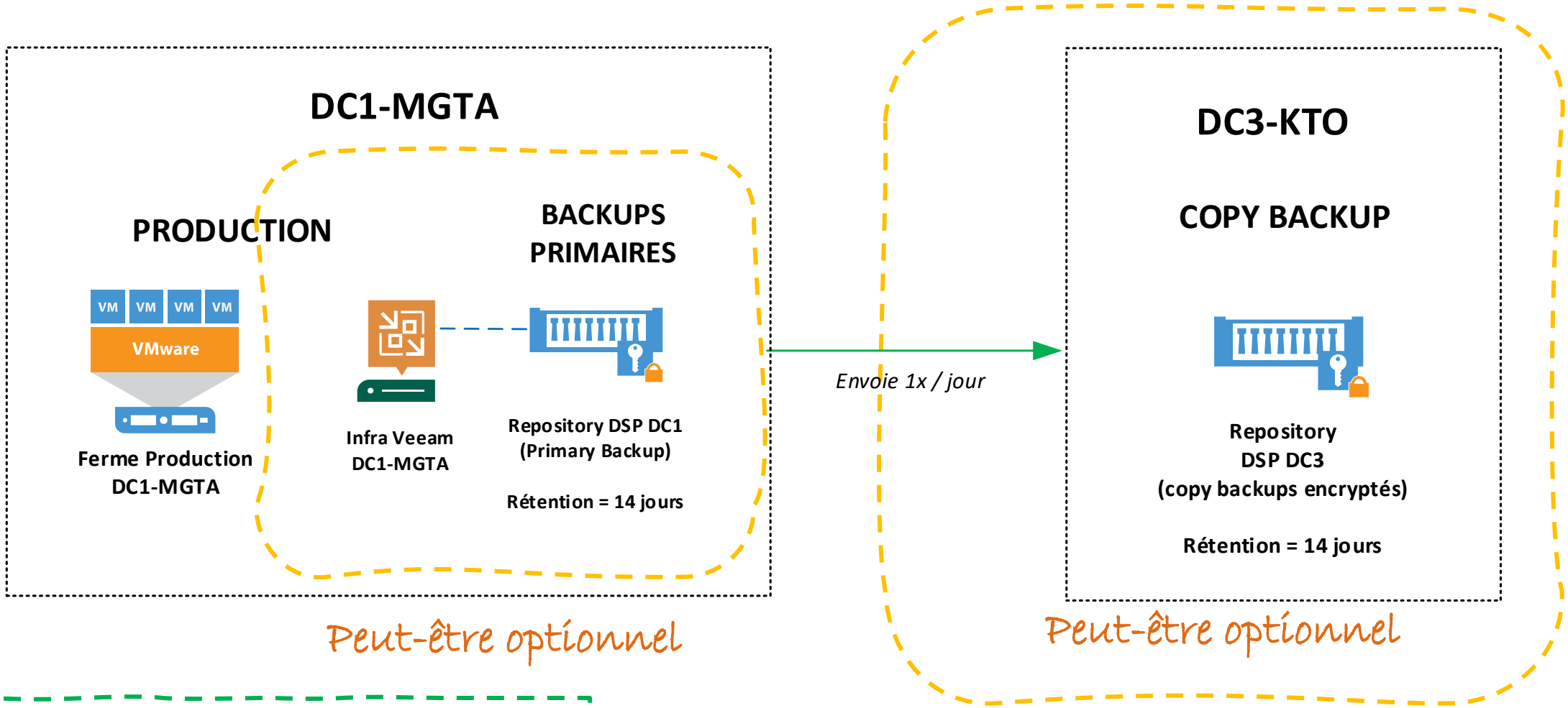
Prestataire prend en charge:

- Les serveurs physiques
- Le stockage
- Le réseau
- La couche de virtualisation
- Garantit sa disponibilité
- Connectivité
- Surveillance et suivi
- Conseils

Des options faciles et rapides :

- Sauvegarde
- PRA
- Infogérance

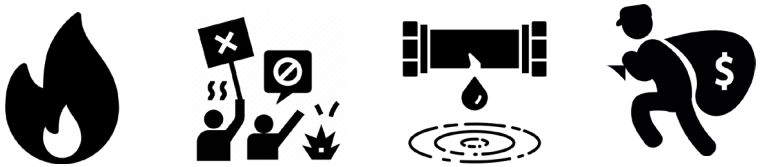
IaaS – Exemple d'infrastructure IaaS



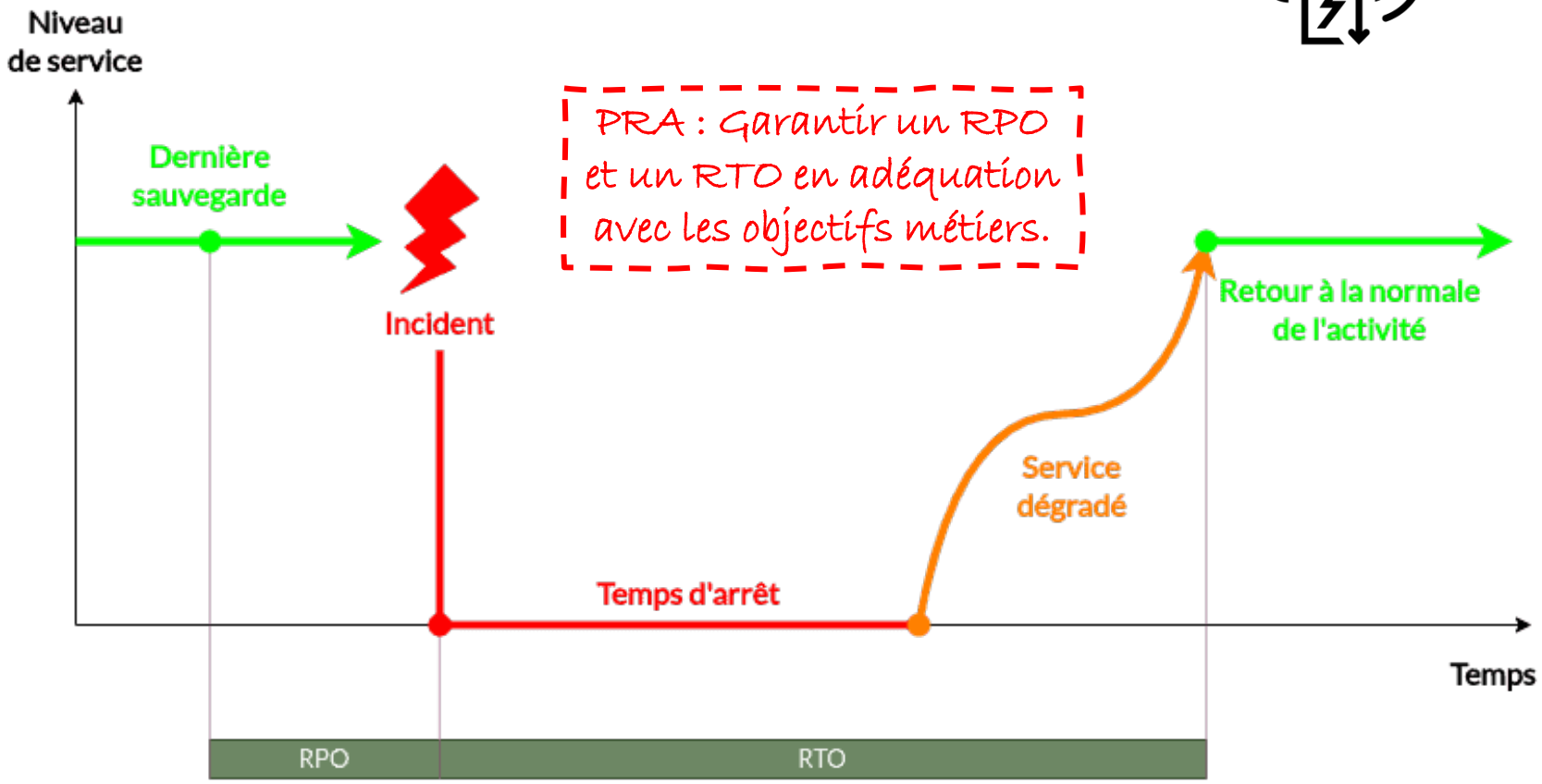
Les infrastructures sont hébergées dans un datacenter offrant les meilleures conditions de sécurité et de disponibilité.

PRA - La reprise après sinistre

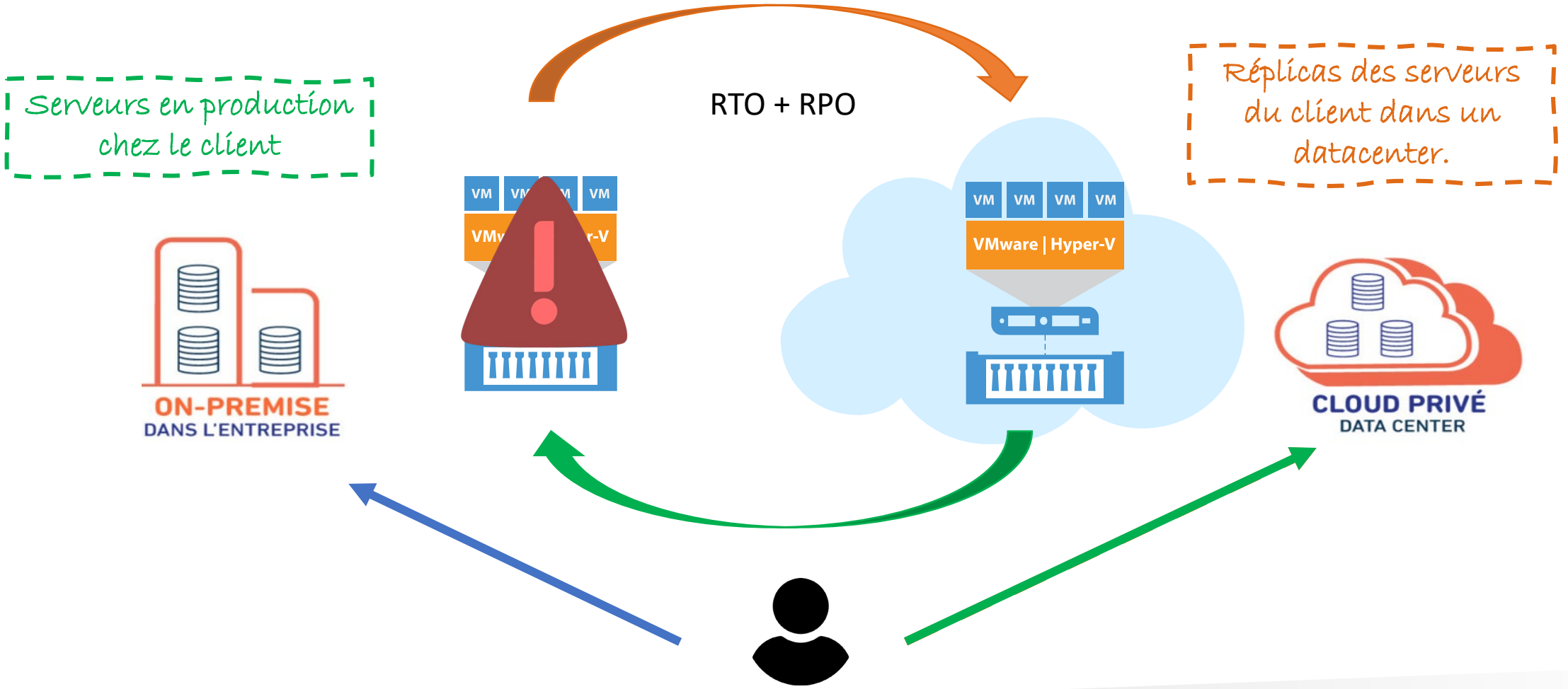
PRA – Objectifs :
Minimiser les temps morts et la perte de données.



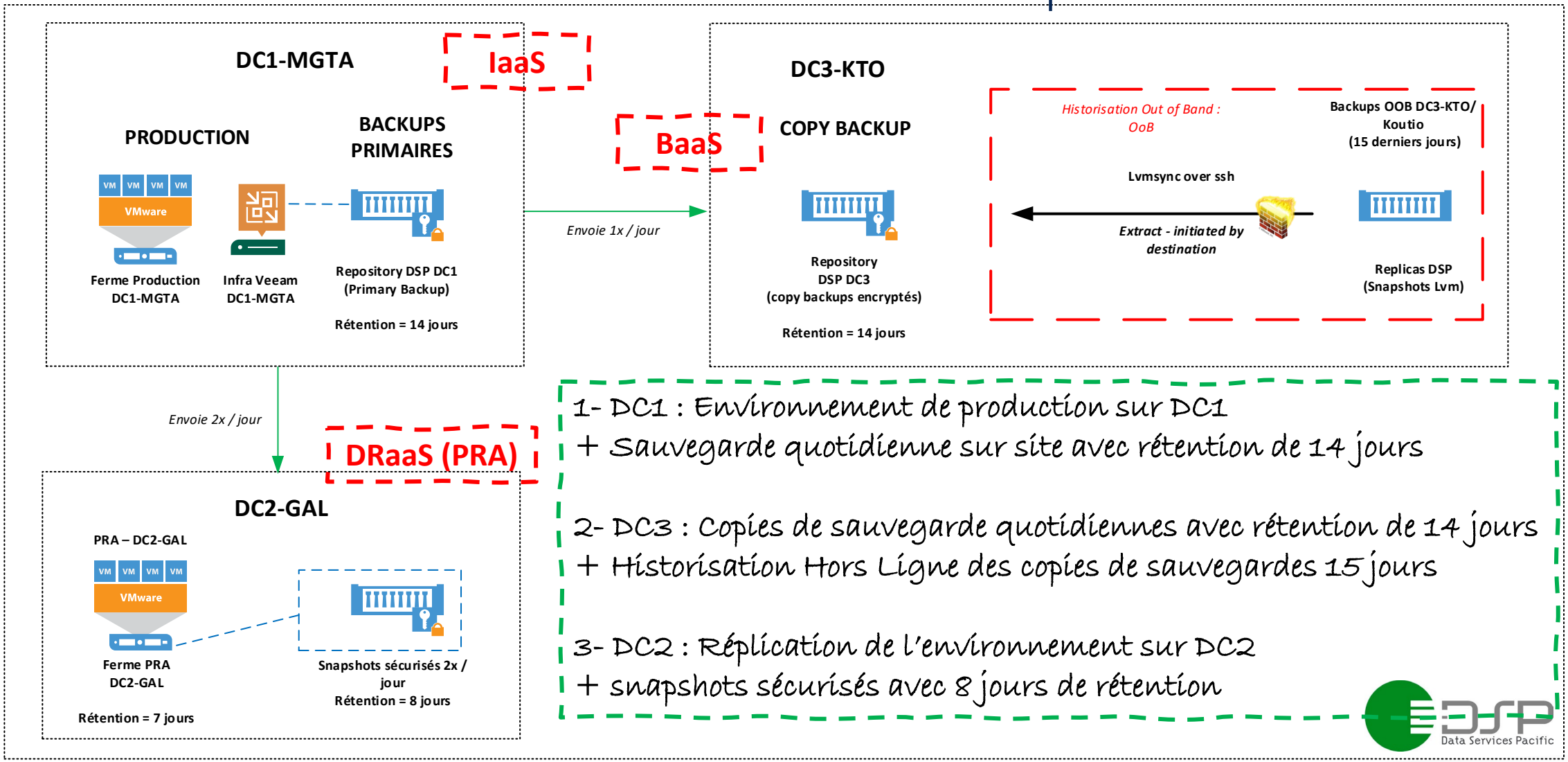
L'objectif premier est de protéger l'organisation dans l'éventualité qu'une partie ou la totalité de ses opérations et services informatiques soit inutilisables.



PRA - La reprise après sinistre : Principe



IaaS + BaaS + DRaaS : Le modèle optimal



cci NOUVELLE-CALÉDONIE

Stocker, sauvegarder et protéger vos données ?

Points de vigilance:

- **La réglementation RGPD → tous les services en ligne ne sont pas conformes**

- **La distance des fournisseurs de services**

- **Les horaires de maintenance des services (décalage horaire)**

- **Le support client pour les services de Cloud Public**

cci NOUVELLE-CALÉDONIE

Réussir sa migration vers le cloud

Par Sylver SCHORGEN

CCI NOUVELLE-CALÉDONIE

Notre agenda

1. Votre speaker
2. Introduction
3. Avantages du Cloud
4. Les risques d’une migration vers le Cloud
5. Planifier sa migration
6. La sécurité des environnements Cloud
7. Quelques mesures de sécurité à mettre en place
8. Conformité & réglementation
9. Questions / Réponses

Qui suis-je ?

Sylver SCHORGEN

Président du Cluster OPEN

CEO du groupe SF2i

Expert en technologie Cloud Microsoft (Microsoft 365 & Azure)

Certifié Microsoft 365 & Ancien Microsoft MVP

15 ans d'expérience sur des projets de migration Cloud

1.

Introduction

Introduction

Le Cloud :

- Composante essentielle dans la **transformation digitale** des entreprises
- Permet de **moderniser l'informatique** des entreprises
- D'accéder à des applications « **à la demande** »
- De réduire certains coûts opérationnels*

Une migration vers le Cloud ne se fait pas sans risque et doit être préparée :

- Définir une **stratégie** de migration
- Faire attention à la **réglementation** et la **conformité**
- S'intéresser à la **sécurité** (durant la migration mais également après)

2.

Avantages & Risques du Cloud

Les avantages du Cloud

Flexibilité et évolutivité : Adaptation rapide aux besoins fluctuants des entreprises.

Rapidité de déploiement : Déploiement quasi instantanée d'application ou de machine virtuelle.

Peu de maintenance : Dans certains types de Cloud (SaaS principalement), il a peu (voir pas) de maintenance technique.

Mobilité & accès global : Accès n'importe où dans le monde depuis une connexion Internet.

Sécurité renforcée : Les fournisseurs Cloud investissent beaucoup dans la cybersécurité, offrant des protections élevées à leurs clients.

Optimisation des coûts* : Les entreprises peuvent économiser certains types de coûts (infrastructure, maintenance, énergie).

Les risques du Cloud

Dépendance à Internet : Pas de connexion Internet, pas de données*

Dépendance au(x) fournisseur(x) : Une fois migré chez un fournisseur, il peut être coûteux d'en changer. Vous êtes également liés à sa politique tarifaire.

Mauvaise configuration : Toute solution Cloud demande de la configuration (notamment pour la partie sécurité).

Sécurité :

- Un hébergeur mutualisé peut être une cible « intéressante » pour des cyber-attaquants
- Mauvaises configurations

Réglementaire & conformité : Réglementation(s) spécifique(s) sur le stockage et l'utilisation des données notamment (RGPD).

3.

Planifier sa migration

Planifier sa migration

1. **Quels sont vos besoins & objectifs**
   a) Réduction des coûts ?
   b) Amélioration des performances ?
2. **Y-a-t'il des contraintes**
   a) Réglementaire ?
   b) Technique ?
3. **Quelles sont vos options / solutions**
   a) Quel type de Cloud (public / privé / hybride)
   b) Quel type de solution (IaaS / PaaS / SaaS)
4. **Élaborer un plan de migration**
   a) Identifiez les applications & les données à migrer
   b) Cartographiez les **dépendances** (entre les applications et les données)
   c) Évaluez **les risques** de votre migration (et les contremesures)

Planifier sa migration

d) **Séquencez** & planifiez votre migration

e) **Validez** votre migration

5. Choisissez votre fournisseur

a) Local (DSP, CSB, MLS, Offratel, ...) ?

b) International (Microsoft, Amazon, Google, OVH, IKOULA, ...) ?

c) Les deux ?

6. Établissez un plan de formation

a) Formation des utilisateurs aux nouveaux usages et outils

7. Établissez un plan de communication

a) Communication avant le démarrage projet

b) Communication pendant le projet

c) Communication en fin de projet

4.

Gestion de la sécurité

Sécurité des environnements Cloud

Responsabilité partagée :

- **Fournisseur *** : Sécurité des infrastructures (datacenters, matériel, les réseaux, …). Il s'assure que les services qu'il fournit sont sécurisés de par leur conception.
- **Client *** : Responsable de la sécurité des données, des accès, et des configurations des services Cloud (mise en œuvre des droits, gestion des utilisateurs, chiffrement des données, la surveillance de la sécurité, …)

Infrastructure as a Service (IaaS) :

- **Fournisseur** : Sécurité physique des datacenters, réseaux, et hyperviseurs.
- **Client** : Sécurité des machines virtuelles, systèmes d'exploitation, données, et applications.

Platform as a Service (PaaS) :

- **Fournisseur** : Sécurité des plateformes, bases de données, et environnements de développement.
- **Client** : Sécurité du code, des applications déployées, des paramètres de bases de données et des données.

Software as a Service (SaaS) :

- **Fournisseur :** Sécurité de l'application
- **Client** : Gestion des utilisateurs, des données et des accès, configuration des paramètres de sécurité.

Quelques mesures de sécurité à mettre en place

La sauvegarde de vos données : Même si les données sont dans le Cloud, elles ne sont pas sauvegardées pas votre fournisseur (sauf accord ou contrat spécifique).

La gestion des mots de passe : Mettez en place une politique de mot de passe stricte avec des mots de passe complexes (minuscules, majuscules, chiffres et symboles).

La gestion de l'authentification : Implémentez le MFA (authentification multifacteur) pour vos utilisateurs.

La gestion de l'accès aux données : Gérez les droits d'accès aux données pour que vos utilisateurs n'accèdent qu'aux données nécessaires pour la bonne exécution de leur travail (principe du moindre privilège).

La sécurité des postes de travail : Vos ordinateurs accèderont à la donnée hébergée, il est donc important qu'ils soient protégés (antivirus, EDR) et à jour.

La sensibilisation à la cybersécurité : Mettez en place des programmes de sensibilisation réguliers de vos collaborateurs ainsi que des tests de sécurité (test de phishing par exemple).

Le chiffrement vos données hébergées : Chiffrez vos données (notamment sensibles) pour empêcher tout accès non autorisés à ces dernières.

5.

Conformité et réglementation

Conformité & Réglementation

Règlement Général sur la Protection des Données (RGPD) : Règlement européen qui s'applique également en Nouvelle-Calédonie. Ce dernier impose des exigences strictes sur la collecte, le traitement, le stockage et la protection des données personnelles.

Réglementation sur les données de santé : Les données de santé doivent être hébergées par des prestataires agréés HDS (Hébergeurs de Données de Santé). Cela inclut des exigences strictes en matière de sécurité physique, logique, et organisationnelle pour protéger les données de santé des patients.

Certifications diverses : En fonction de votre métier, il peut être obligatoire pour vous que votre hébergeur dispose de certification (ISO, ...).

MERCI DE VOTRE ATTENTION

CCI NOUVELLE-CALÉDONIE