WORKSHOP

Du Backup au Plan de Continuité : Quelles solutions pour la continuité de votre IT ?

DFi Data First
GROUPE CHEOPS TECHNOLOGY

Hewlett Packard Enterprise

ABILENE ADVISORS

Qui sommes-nous ?

DFi Data First
GROUPE CHEOPS TECHNOLOGY

48 Collaborateurs

Hewlett Packard Enterprise Silver Partner

10 M de CA

CHEOPS TECHNOLOGY
The Cloud Customized For You !

700 Collaborateurs

Hewlett Packard Enterprise Platinum Partner

160 M de CA

Qui sommes-nous ?

CLOUD & SERVICES MANAGÉS

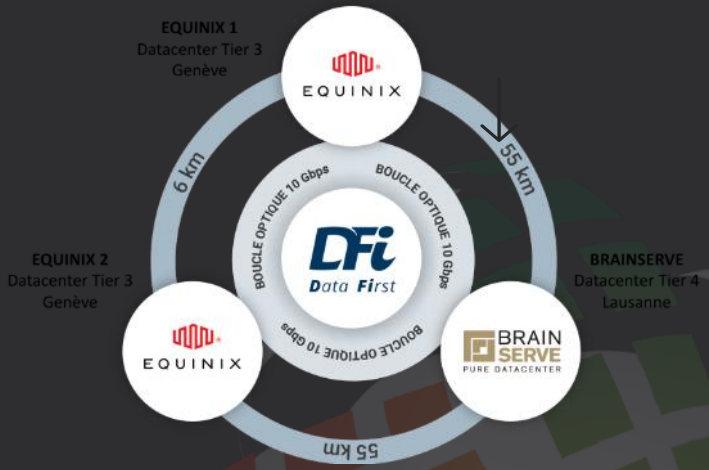
CYBERSÉCURITÉ

RÉSEAUX & COMMUNICATIONS UNIFIÉES

MODERNISATION TECHNOLOGIQUE

3 Datacenters

Equinix 1, Equinix 2 et Brainserve



1 PetaByte de Données

2 Petabytes de Backup

Welcome

8:00 **Accueil & Café**

ABILENE ADVISORS

8:30 **Environnement et régulations : vers toujours plus de résilience opérationnelle?**

Jean-Luc Affaticati - Directeur

DFi Data First – Groupe Cheops Technology

Hewlett Packard Enterprise

9:30 **Quelles solutions pour la continuité de votre IT ? & Cas Pratiques**

Vincent Evrard - Avant-Vente DFi Service

Hervé Gaudin - Senior Storage Technology Consultant HPE

10:30 **Discussion - Q&A**

Avec tous nos experts

Reprise des activités après un sinistre

Environnement et règlementation: vers toujours plus de résilience opérationnelle?

ABILENE ADVISORS

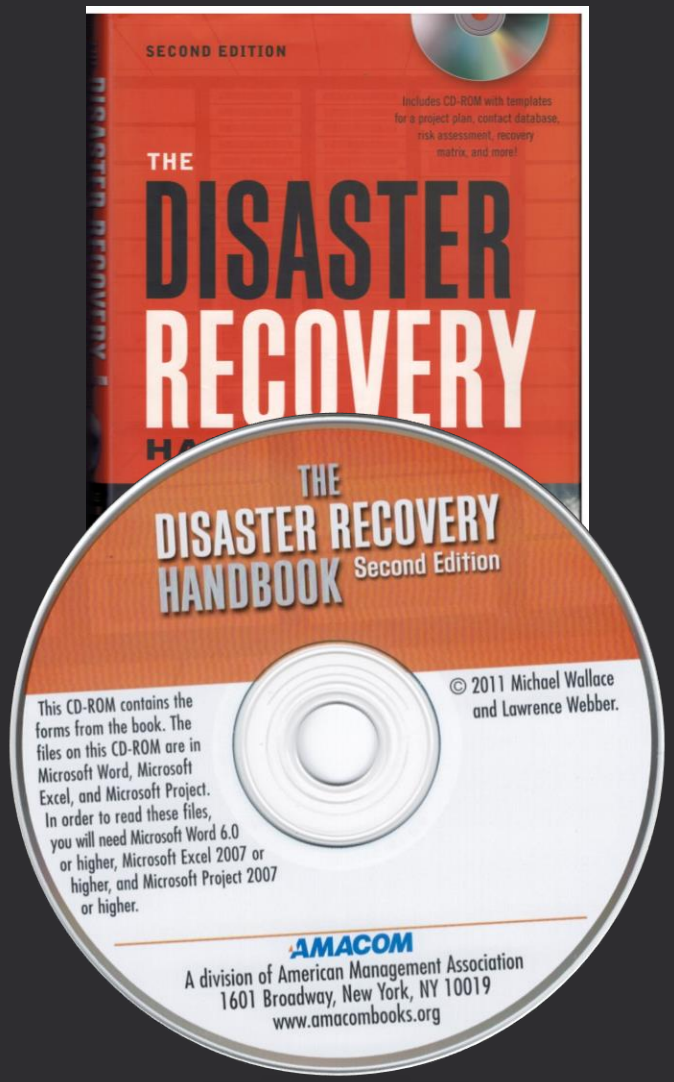
Société de conseils

- Evaluer, Construire, Améliorer

Gouvernance

- Sécurité
- Données Personnelles
- Continuité
- Risques
- Conformité
- Intelligence Artificielle

2011



Évaluation des Risques	Identification des actifs critiques et évaluation des risques susceptibles d'affecter ces actifs
Stratégies de Redondance	Mise en place de redondances pour les systèmes critiques et la réplication de données.
Planification et Documentation	Élaboration de procédures détaillées pour la réponse aux incidents et la reprise des activités, y compris les rôles et les responsabilités.
Formation et Sensibilisation	Formation régulière des employés aux procédures du plan de continuité et réalisation d'exercices de simulation.
Tests et Révisions	Tests périodiques du plan pour s'assurer de son efficacité et mise à jour continue pour s'adapter aux changements organisationnels ou technologiques.
Communications	Développement de protocoles de communication pour les parties prenantes en cas d'interruption des activités.
Reprise des Opérations	Établissement de procédures pour restaurer rapidement les opérations après un sinistre.

2024

Apport de la technologie	
Automatisation et Orchestration	L'automatisation évite les erreurs humaines.
Cloud et Multi-Cloud	Le multi-cloud comme résilience aux risques cloud ;-)
Virtualisation	Capacité à la demande
Cyber-résilience	Détection et réponse aux cyberattaques font partie du plan
Intelligence Artificielle (IA) et Machine Learning	Prévention, détection, optimisation de la réponse et de la reprise
Tests Continus	Tests de reprise continus et automatisés

Facteurs de complexité (n!)	
Complexité des Infrastructures	Environnements informatiques hétérogènes, clouds hybrides et multi-clouds
Volume de Données	Volumes exponentiels de sauvegarde et de restauration
Menaces de Sécurité Evolutives	Sophistication croissante des cybermenaces exigent des plans de reprise plus fins
Dépendance aux Fournisseurs	Dépendance à des tiers pour les services critiques
Conformité et Réglementation	Alignement des technologies émergentes avec les exigences réglementaires en évolution
Interconnexion des Systèmes	Interconnexion entre eux, avec l'IoT et d'autres technologies émergentes.


Que s’est-il passé?

Principales régulations (EU)

Quel impact sur la reprise opérationnelle ?

EU	
RGPD	Mai 2018
NIS2*	Octobre 2024
DORA	Janvier 2025
AI Act	2026 (publication + 2 ans)

(*: NIS Août 2016)

RGPD (Règlement général sur la protection des données)

- Mesures de sécurité
  - Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données
- Considérations pour la mise en œuvre
  - le RGPD (art. 32) ne fournit pas de directives détaillées sur la manière dont ces exigences doivent être mises en œuvre…

ABILENE ADVISORS

NIS2 (Network and Information Systems Directive)

- Analyse des risques et de la sécurité des systèmes d'information;
- Traitement et gestion des incidents;
- Continuité des activités,
  - gestion des sauvegardes
  - reprise après sinistre
  - gestion de crise
- Evaluation de l'efficacité des mesures de gestion des risques liés à la cybersécurité

Consid. (79): conformément à ISO 27000

Art. 25 al.1 : normes techniques internationales

DORA (Digital Operational Resilience Act)

- Tests de résilience opérationnelle informatique
  - Les entités financières doivent s’assurer qu’elles peuvent résister, répondre et se rétablir face à toute perturbation opérationnelle grave liée aux technologies de l’information et de la communication
- Mesures de protection contre les menaces potentielles dues à des erreurs humaines et à une administration inadéquate
- Gouvernance de la gestion des risques informatiques

Le Swiss finish

Principales régulations CH

L’arsenal est +/- en place à ce jour

Implication sur la reprise opérationnelle ?

EU		Suisse	
RGPD	Mai 2018	LPD	Septembre 2023
NIS2	Octobre 2024	LSI	Janvier 2024 (+)
DORA	Janvier 2025	FINMA 23/01	Janvier 2024
AI Act	(2026)	Quelle IA?	

Data Protection en Suisse, LPD, LIPDA, LIPAD et autres

Mesures de Sécurité

- Mettre en œuvre les mesures techniques et organisationnelles appropriées
- Assurer un niveau de sécurité adéquat au risque
- Protection contre le traitement non autorisé ou illégal, la perte, la destruction ou les dommages accidentels.

Gestion des Risques

- Evaluation et gestion des risques
- Mesures de mitigation appropriées, y compris des plans de disaster recovery.

Continuité des Affaires

- La continuité des affaires est une obligation de protéger les données personnelles
- Les opérations liées au traitement des données peuvent continuer et les données peuvent être restaurées en cas de sinistre.

(cadre 27701)

LSI (Loi Fédérale sur la sécurité de l'information)

- Planification de la Continuité des Activités (PCA)
- Procédures de sauvegarde des Données
- Redondance des Systèmes
- Centres de Données de Secours
- Tests et Exercices de Simulation
- Formation du Personnel sur les procédures de disaster
- Audit et Révision des Mesures

(mais rien encore sur les entités critiques)

(cadre 27001)

FINMA 2023/01 (Risques et résilience opérationnels – banques)

DORA un an avant DORA

- **Gestion globale des risques opérationnels**
  - Identification, évaluation, limitation et surveillance des risques opérationnels.
- **Risques TIC**
- **Risques cyber**
- **Risques liés aux données critiques**
  - Gestion des risques associés aux données qui sont d'une importance cruciale pour l'institution.
- **Gestion de la continuité des activités (BCM)**
  - Préparation et planification pour assurer la continuité des opérations en cas de perturbation majeure.

Et bien plus encore…

(cadre 27001 + 22301)

La grande famille des régulations de résilience opérationnelle

Tous ces éléments constituent le cœur des contrôles relatifs à la gestion de la continuité d'activité et de la reprise des activités.

Ils se parent des couleurs de votre industrie.

Ils visent à préparer l'organisation à réagir efficacement à des incidents et à des désastres pour minimiser les impacts sur les opérations.

Et il paraîtrait que la menace augmente.

ISO 22301 – la mère de tous les systèmes de continuité ?

- **Évaluation des risques et continuité d’activité**
  - **Identifier les risques** qui peuvent affecter la capacité de l'organisation à opérer.
  - **Déterminer les fonctions critiques** de l'organisation et les ressources nécessaires pour les soutenir.
- **Stratégies de continuité d’activité**
  - Développer des **stratégies** pour assurer la continuité des opérations critiques et la reprise après sinistre.
- **Plans de réponse à l’incident**
  - Établir des **plans de réponse** spécifiques pour gérer différents types d'incidents, y compris les désastres.
- **Tests, maintenance et revue**
  - **Tester et réviser régulièrement** les plans de continuité d'activité et de disaster recovery pour s'assurer qu'ils restent pertinents et efficaces.
- **Formation et sensibilisation**
  - Assurer que le personnel est **formé et conscient** de leurs rôles et responsabilités en matière de continuité d'activité et de reprise après sinistre.

Merci

ABILENE ADVISORS

Jean-Luc AFFATICATI

jean-luc.affaticati@abileneadvisors.ch






Florilège d'IA dégénérative




(cadre 42001)

Quelles solutions pour la continuité de votre IT ?

Qui sommes-nous ?

Vincent Evrard

Ingénieur Avant-Vente

Hervé Gaudin

Senior Storage Presales & Technology Consultant

DFi Data First
GROUPE CHEOPS TECHNOLOGY

Hewlett Packard Enterprise

Infrastructure Simple

Protection :

Aucune !

Infrastructure avec Backup Simple

Protection :

- ☒ PROBLÈMES HARDWARE
- ☑ PROBLÈMES SOFTWARE
- ☑ PROBLÈMES HUMAINS
- ☒ PROBLÈMES DE VIRUS (RANSOMWARES)
- ☒ DÉSASTRES

Infrastructure Redondante ou Cloud

Protection :

- ☑ PROBLÈMES HARDWARE
- ☑ PROBLÈMES SOFTWARE
- ☑ PROBLÈMES HUMAINS
- ☒ PROBLÈMES DE VIRUS (RANSOMWARES)
- ☒ DÉSASTRES

Infrastructure avec Backup Externalisé

Protection :

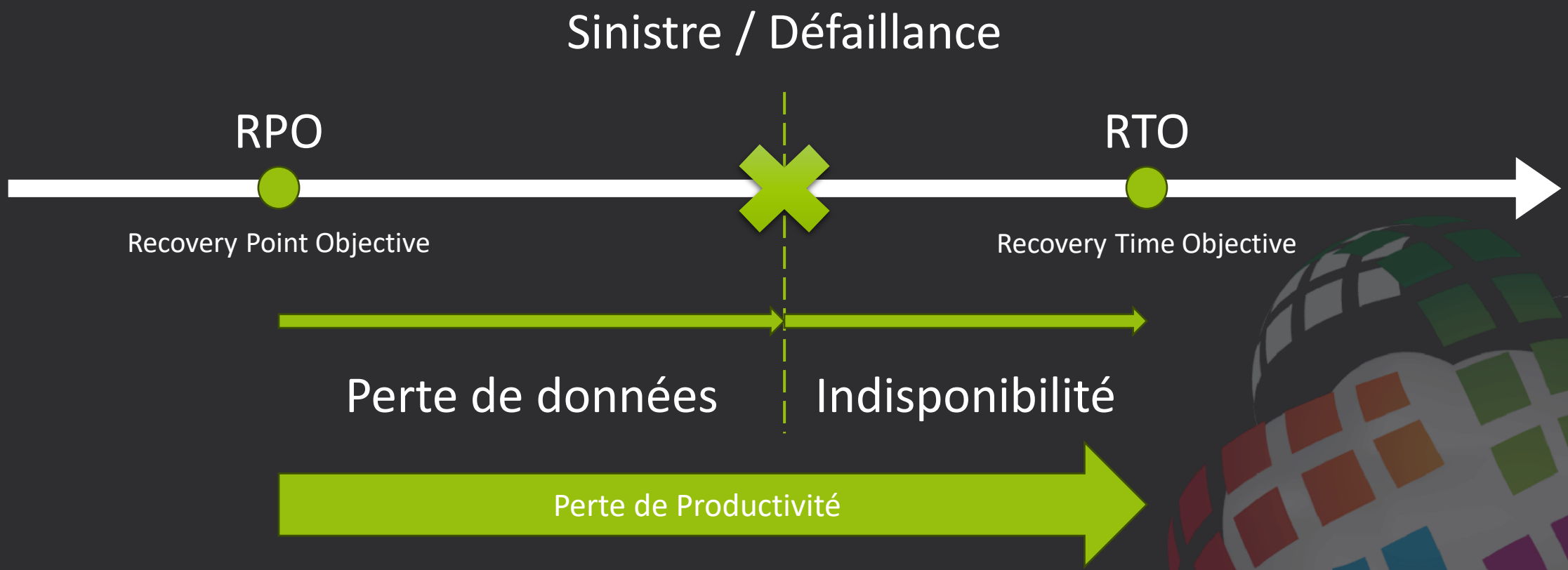
- [x] PROBLÈMES HARDWARE
- [x] PROBLÈMES SOFTWARE
- [x] PROBLÈMES HUMAINS
- [ ] PROBLÈMES DE VIRUS (RANSOMWARES)
- [x] DÉSASTRES

Infrastructure avec Backup Immuable

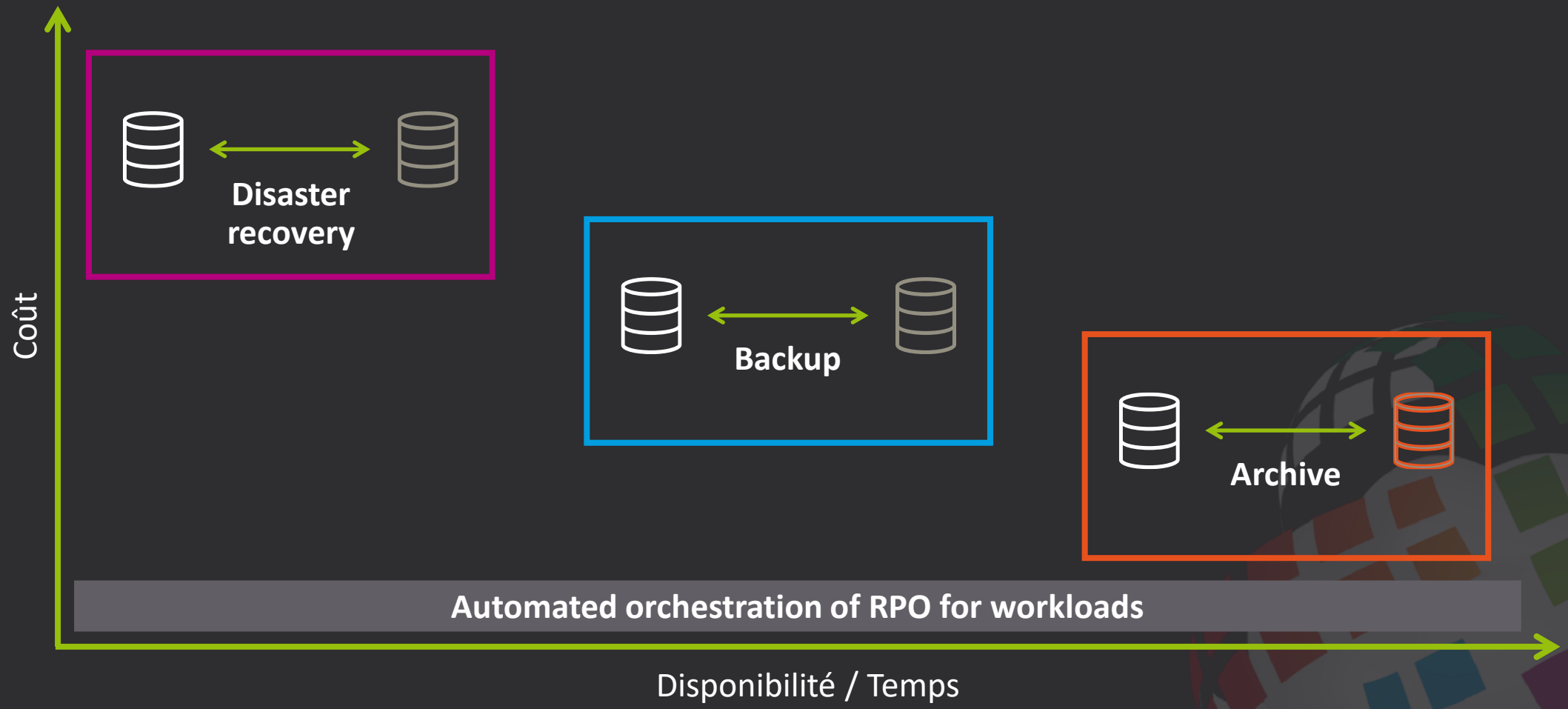
Protection :

- ☑ PROBLÈMES HARDWARE
- ☑ PROBLÈMES SOFTWARE
- ☑ PROBLÈMES HUMAINS
- ☑ PROBLÈMES DE VIRUS (RANSOMWARES)
- ☒ DÉSASTRES

RPO/RTO



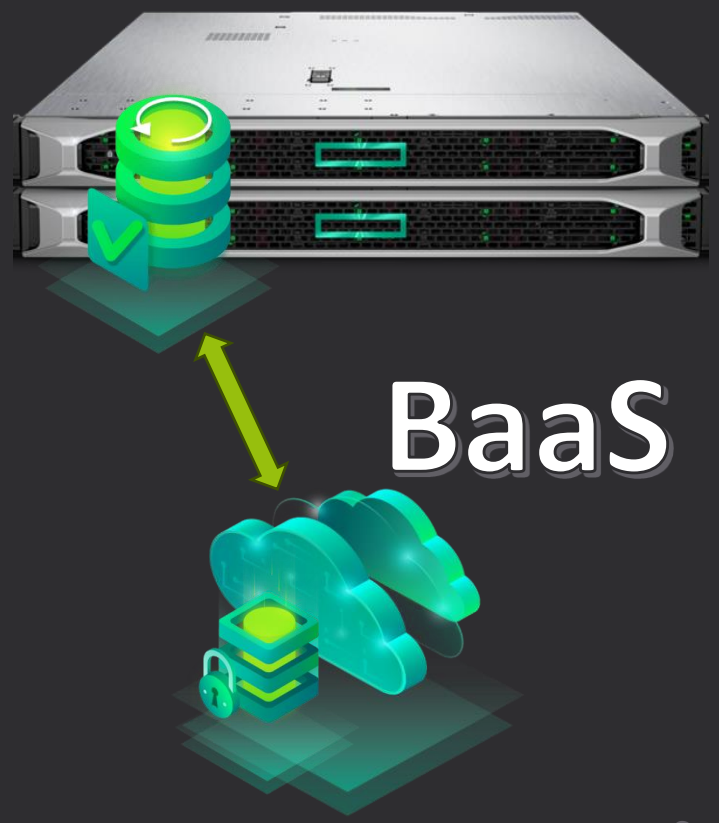
Quelle protection choisir ?



Cas Clients

Cas 1: Externalisation de Backup Immuable

Cas 1: Externalisation de Backup Immuable



Protection :

- PROBLÈMES HARDWARE
- PROBLÈMES SOFTWARE
- PROBLÈMES HUMAINS
- PROBLÈMES DE VIRUS (RANSOMWARES)
- DÉSASTRES

Cas 1: Externalisation de Backup Immuable

RPO	RTO*
0	>=0
24H	2 à 4H
24H	2 à 4H
24H	>24H
24H	>48H

Protection :

- PROBLÈMES HARDWARE
- PROBLÈMES SOFTWARE
- PROBLÈMES HUMAINS
- PROBLÈMES DE VIRUS (RANSOMWARES)
- DÉSASTRES

*Dépendant de la volumétrie et de la bande passante

Cas 2: Besoin de confiance dans son IT

Cas 2: Besoin de confiance dans son IT

Situation Actuelle

RPO	RTO*
0	>=0
24H	2 à 4H
24H	2 à 4H
24H	>24H
NA	NA

Protection :

- ☑ PROBLÈMES HARDWARE
- ☑ PROBLÈMES SOFTWARE
- ☑ PROBLÈMES HUMAINS
- ☑ PROBLÈMES DE VIRUS
- ☒ DÉSASTRES

*Dépendant de la volumétrie

Cas 2: Besoin de confiance dans son IT

Expression du besoin

Situation actuelle :

Besoin:

RPO	RTO*	PROTECTION	RPO	RTO*
0	>=0	HARDWARE	0	>=0
24H	**2 à 4H**	SOFTWARE	**24H**	**2 à 4H**
24H	**2 à 4H**	HUMAIN	**24H**	**2 à 4H**
24H	**>24H**	VIRUS (RANSOMWARE)	**24H**	**NBD**
NA	**NA**	DÉSASTRE	**24H**	**NBD**

*Dépendant de la volumétrie

Cas 2: Besoin de confiance dans son IT

Réponse

SITE DE PRODUCTION

SITE DE DÉSASTRE

DRaaS

Azure

aws

CLOUD PUBLIC

INFRASTRUCTURE ON-PREMISE

iCOD

Energy Min Power Max !

CLOUD PRIVÉ MUTUALISÉ

	RTO	DRP	RTO*
DÉSASTRE	> 48H	→	NBD

*Dépendant de la volumétrie

Cas 2: Besoin de confiance dans son IT
Réponse

PROTECTION	RPO	RTO*
HARDWARE	0	>=0
SOFTWARE	**24H**	**2 à 4H**
HUMAIN	**24H**	**2 à 4H**
VIRUS (RANSOMWARE)	**24H**	**NBD**
DÉSASTRE	**24H**	**NBD**

*Dépendant de la volumétrie

Cas 3: Cas client « Grande Distribution »

Cas 3: Cas client « Grande Distribution »

Situation Actuelle

SITE DE PRODUCTION

SITE DE DÉSASTRE

Cas 3: Cas client « Grande Distribution »

Expression du Besoin

Situation actuelle :

RPO	RTO*
0	0
4H	8H
4H	8H
4H	8H
NA	NA
NA	NA

*Dépendant de la volumétrie

PROBLÈMES HARDWARE

PROBLÈMES SOFTWARE

PROBLÈMES HUMAINS

DÉSASTRES

PROBLÈMES DE VIRUS

BACKUP « LEGAL »

Besoin:

RPO	RTO*
0	0
4H	8H
4H	8H
4H	8H
4H	8H
1 an	NA

Cas 3: Cas client « Grande Distribution »

Réponse

SITE DE PRODUCTION

SITE DE DÉSASTRE

INFRASTRUCTURE ON-PREMISE

Cas 3: Cas client « Grande Distribution »

Réponse

Besoin:

RPO	RTO*
0	0
4H	8H
4H	8H
4H	8H
4H	8H
1 an	NA

PROBLÈMES HARDWARE

PROBLÈMES SOFTWARE

PROBLÈMES HUMAINS

DÉSASTRES

PROBLÈMES DE VIRUS

BACKUP « LEGAL »

Situation finale:

RPO	RTO*
0	0
4H	8H
4H	8H
4H	8H
4H	8H
1 an	NA

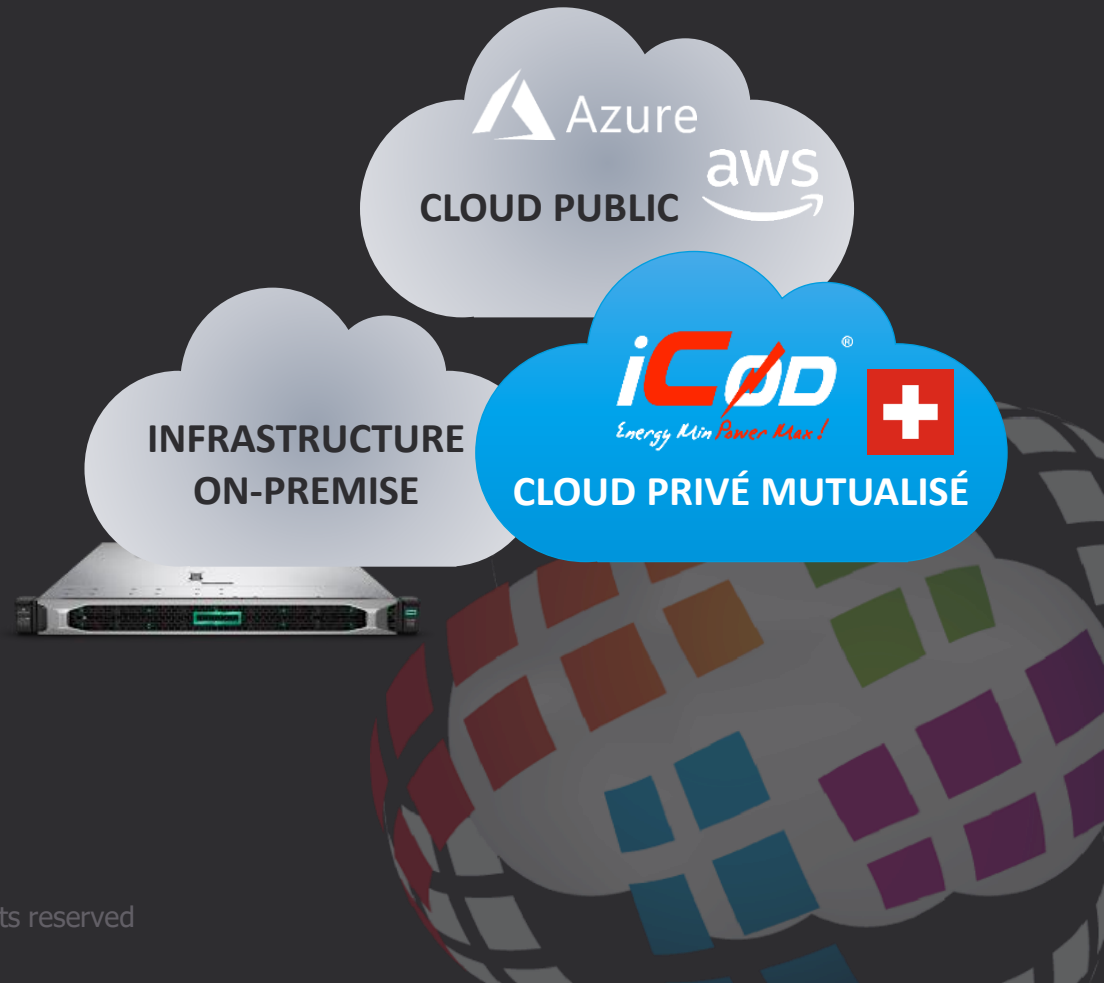
*Dépendant de la volumétrie

Cas 4: Cas de Business Continuity

Cas 4: Cas de Business Continuity
Situation Actuelle

SITE DE PRODUCTION

SITE DE DÉSASTRE



Cas 4: Cas de Business Continuity
Agir sur le RPO

	RPO
PROBLÈMES HARDWARE	0
PROBLÈMES SOFTWARE	24H
PROBLÈMES SOFTWARE	24H
PROBLÈMES DE VIRUS (RANSOMWARES)	24H
DÉSASTRES	24H

Sauvegardes ⊕ fréquentes
→ Snapshots
OU
Journaling

Cas 4: Cas de Business Continuity
Réponse

SITE DE PRODUCTION

SITE DE DÉSASTRE

CDP

Azure

aws

CLOUD PUBLIC

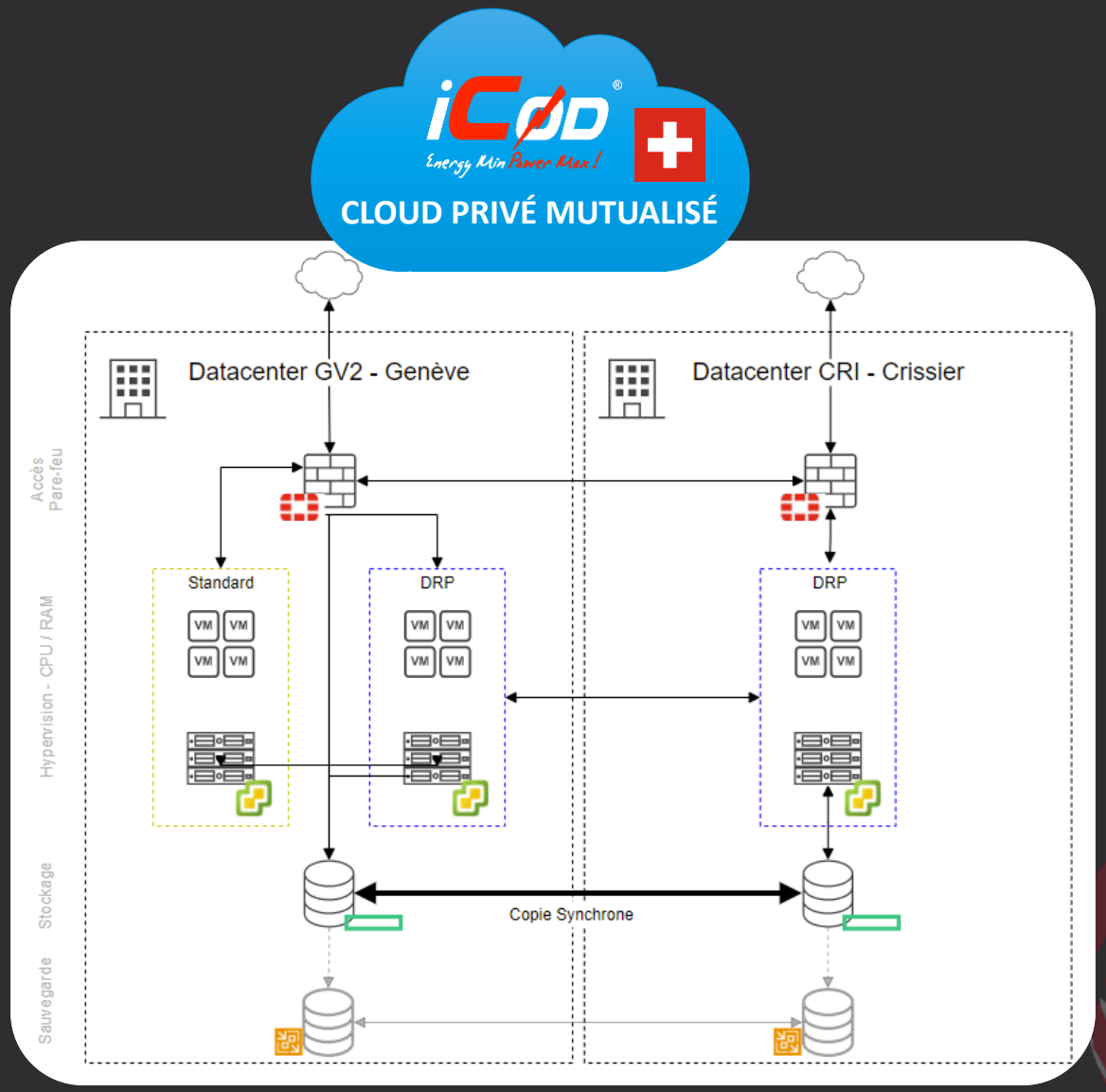
INFRASTRUCTURE
ON-PREMISE

iCOD
Energy Min Power Max !

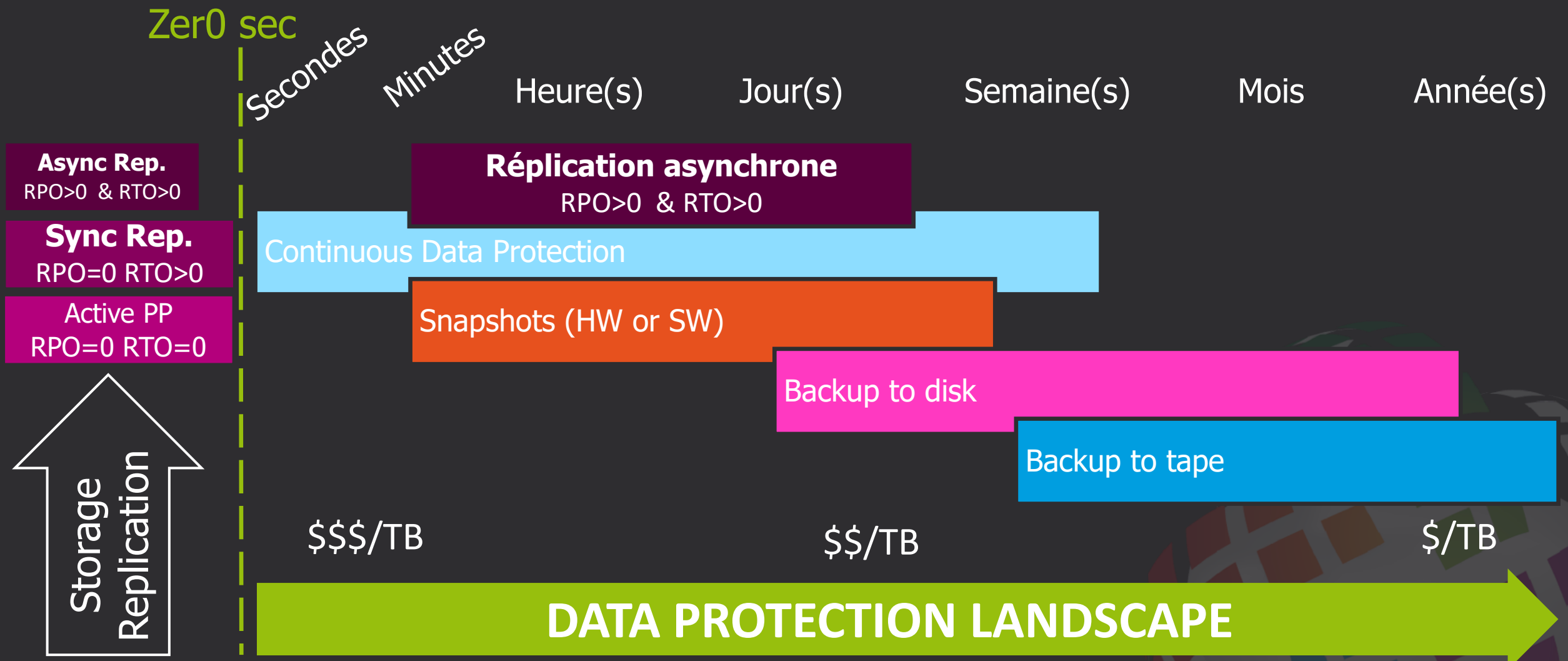
CLOUD PRIVÉ MUTUALISÉ

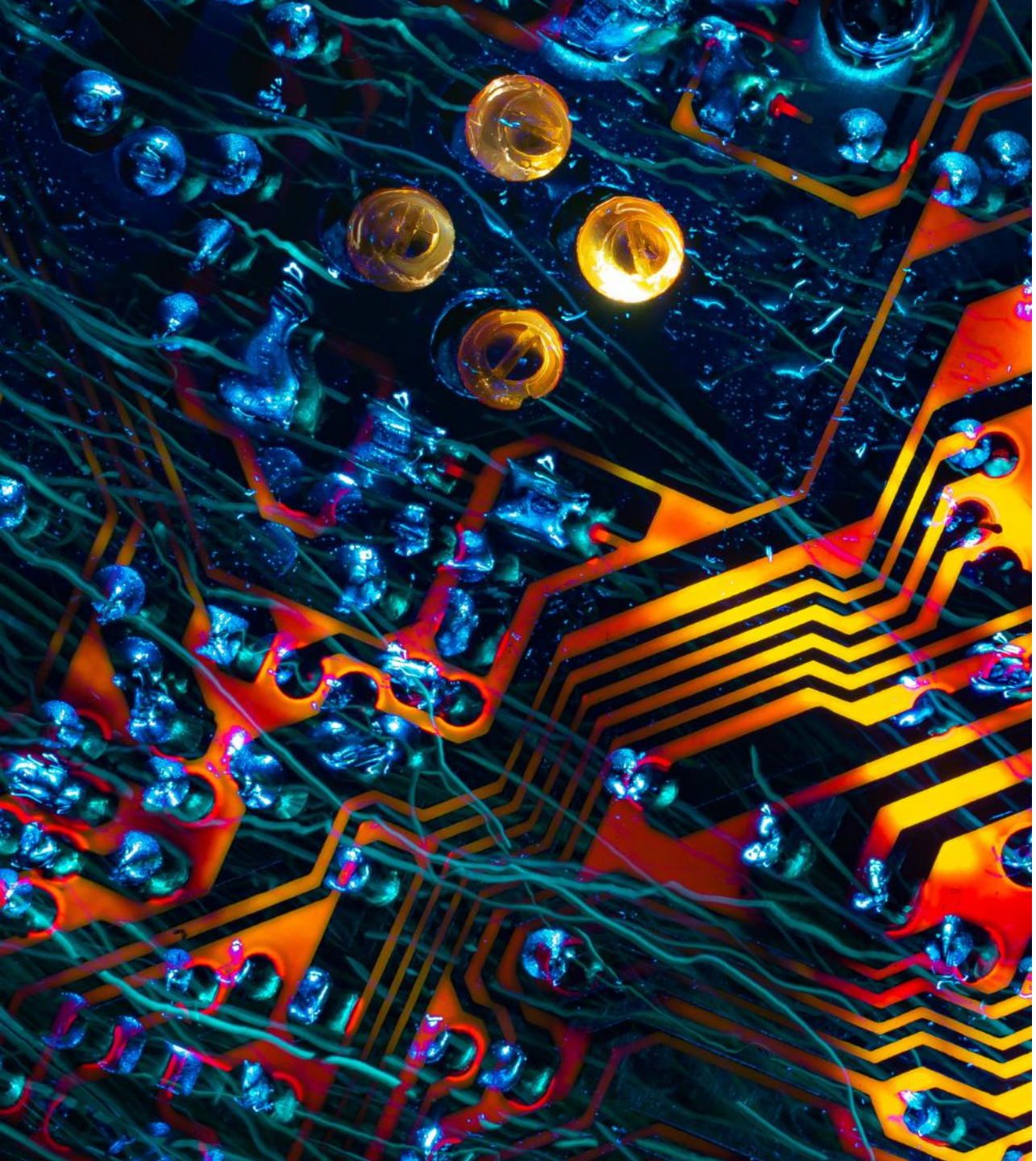
Cas 4: Cas de Business Continuity

Réponse

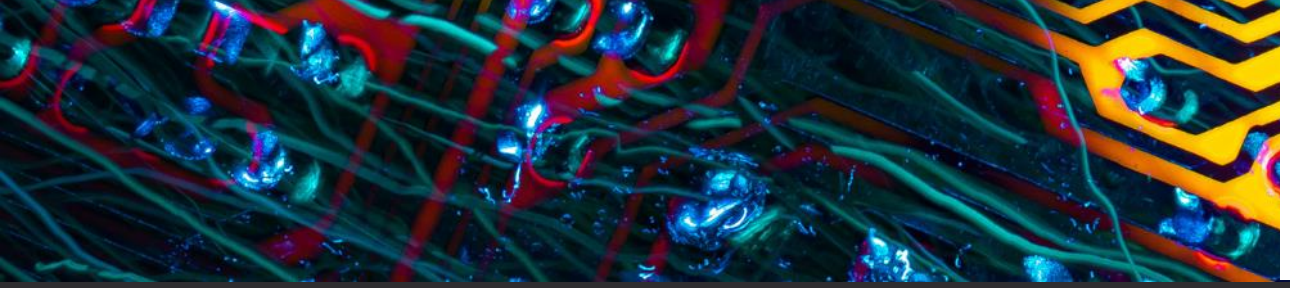


En résumé…





MERCI



Des questions ?