Comment vous préparer au mieux pour faire face aux imprévus ?

L'essentiel à connaître en matière de protection et de sauvegarde des données

Maîtrisez la protection de vos données

La protection
c'est assurer la confidentialité, l'intégrité et la disponibilité des données.

La sauvegarde
permet d'assurer la disponibilité et la récupération des données en cas de besoin.

Les niveaux de maturité

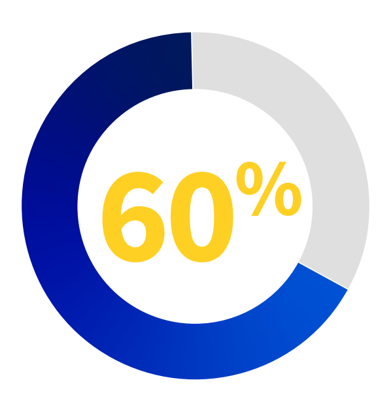
Si ce processus nécessite réflexion, temps et investissement, vous pouvez progresser à votre rythme, grâce à la mise en place d'actions adéquates et ciblées.

0 INEXISTANT	1 INFORMEL	2 RÉPÉTABLE	3 DÉFINI	4 CONTRÔLÉ	5 OPTIMISÉ
Tout est à faire	Imprévisible, incohérent et à haut risque	Réactif, instable et manuel	Documenté, standardisé et révisable	Proactif, monitoré et légèrement automatisé	Automatisé, intégré et prévisible

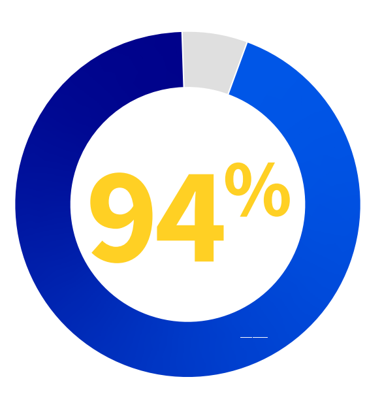
Downtime & Loss

Avec une croissance exponentielle du volume des données et de plus en plus d'entreprises qui se déclarent « data driven », les risques n'ont jamais été aussi élevés.

LA QUANTITÉ DE DONNÉES DOUBLE ENVIRON TOUS LES DEUX ANS.[1]



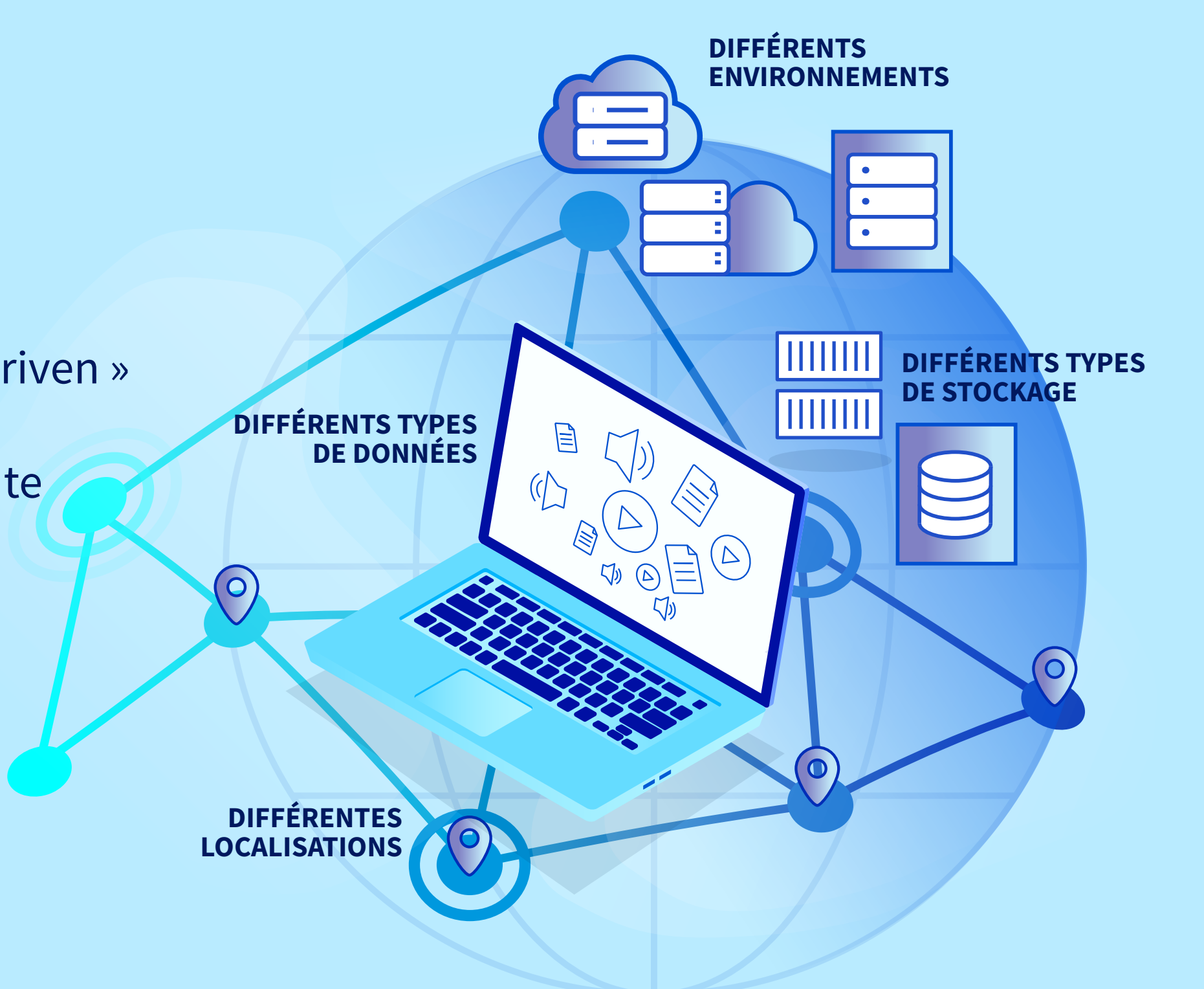
60% DES ENTREPRISES ONT PRIS DES MESURES POUR ÊTRE « DATA DRIVEN ».[2]



94% DES ENTREPRISES ONT SIGNALÉ DES INDISPONIBILITÉS NON PRÉVUES.[2]

Un sujet de plus en plus complexe

Les organisations « data driven » sont confrontées à une complexité croissante en matière de protection des données et de reprise après sinistre.



Plus qu'une vue de l'esprit, une réalité !

Les menaces pesant sur les données ont tendance à se multiplier et à s'intensifier. Et lorsque celles-ci surviennent, les conséquences tendent à s'aggraver.

Au cours de l'année 2021

93% des entreprises ont subi une interruption d'activité liée aux données.[2]

68% des personnes interrogées ont subi au moins 4 interruptions de ce type.[2]

83% ont indiqué qu'au moins une attaque avait entraîné la corruption de données.[2]

60% ont été confrontées à des données irrécupérables.[2]

2,3 **INTERRUPTIONS** en moyenne par mois[4]

5,1 **HEURES** durée moyenne entre le début de l'interruption et le rétablissement des services[4]

D'où proviennent les menaces ?

Qu'elles soient internes ou externes, les sources sont multiples.

ATTAQUES DDOS
ransomwares
CYBERATTAQUES
malwares virus
DÉFAILLANCES MATÉRIELLES **phishing** PANNES
SURCHAUFFES
problèmes d'alimentation

perte de **matériel**
vol de matériel
fuites d'informations internes
ERREURS HUMAINES ACCÈS NON AUTORISÉS
mauvaises configurations
politiques de sécurité inadéquates
INONDATIONS tremblements **de terre**
CATASTROPHES NATURELLES incendies
ouragans FAUNE

23% **Les erreurs humaines** sont la première cause des incidents de violation de données.[3]

x2,5 **Les ransomwares** sont plus susceptibles de provoquer un sinistre qu'une catastrophe naturelle.[2]

62% **L'augmentation** des attaques par ransomware dans le monde en 2020 par rapport à 2019.[5]

2 **Les principales causes** de reprise après sinistre : les défaillances logicielles à 56 % et matérielles à 47 %.[2]

1er **Le défi majeur,** c'est la fiabilité des opérations de sauvegarde et récupération.[2]

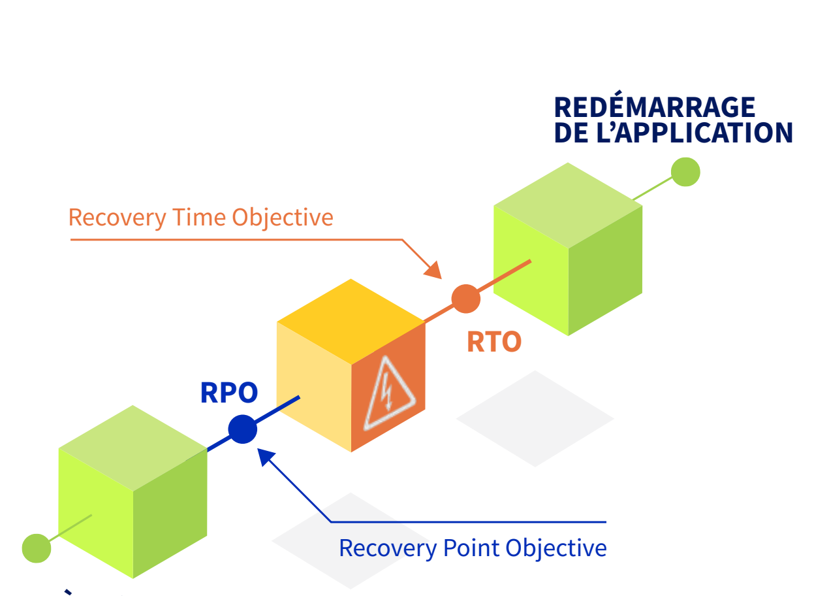
La stratégie de sauvegarde 3-2-1

- **Créez 3 copies de vos données**, soit l'original et 2 copies de sauvegarde.
- **Stockez-les sur 2 supports différents** : disque et/ou bande sur site distant, stockage dans le cloud, etc.
- **Maintenez 1 copie hors ligne** sur 1 stockage déconnecté du réseau ou 1 support de stockage amovible.

La stratégie complète de protection des données :

1. Évaluer tous les risques
Identifiez l'ensemble des menaces auxquelles votre organisation pourrait être confrontée ainsi que les données les plus sensibles/critiques.

2. Définir les objectifs associés
Que faut-il mettre en place pour assurer la continuité de votre activité (PCA) ?
En cas d'arrêt, quels seraient les objectifs de délai de reprise (RTO) et de perte de données maximale (RPO) pour vos systèmes et applications, en distinguant ceux qui sont non critiques, essentiels et critiques ?



3. Élaborer une stratégie sur mesure
Choisissez une stratégie de reprise après sinistre adéquate (scénario à froid, tiède ou à chaud) ou optez pour un plan de reprise d'activité (PRA) dans le cloud pour bénéficier de ses avantages.

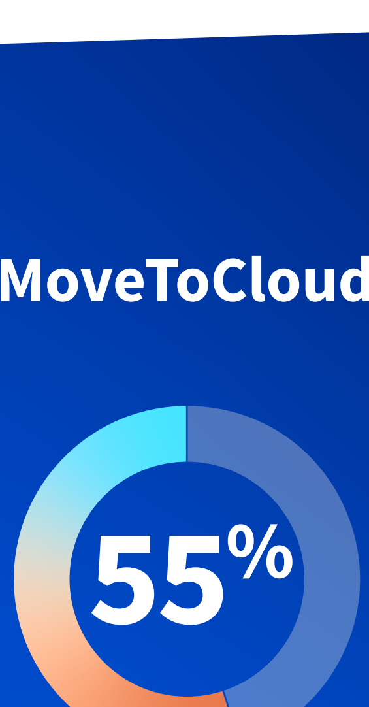
4. Tester et répéter
Vérifiez régulièrement que votre stratégie est toujours adaptée à vos besoins et assurez-vous également de son efficacité.

5. Documenter les procédures
Renseignez clairement et précisément chaque aspect de votre PRA, y compris les procédures de réponse, la communication et la récupération du système.

6. Former et informer vos collaborateurs
N'oubliez pas de sensibiliser vos collègues aux bonnes pratiques en matière de sécurité informatique.

7. Surveiller, maintenir et mettre à jour
Soyez prêts à détecter toute activité suspecte pour réagir rapidement et efficacement. Révisez et mettez à jour régulièrement votre PRA afin d'en garantir la pertinence et faire face aux attaques et aux problèmes émergeants.

#MoveToCloud



55% DES ENTREPRISES AURONT ADOPTÉ UNE STRATÉGIE DE PROTECTION DES DONNÉES DANS LE CLOUD, D'ICI 2025.[2]

Avant de migrer :

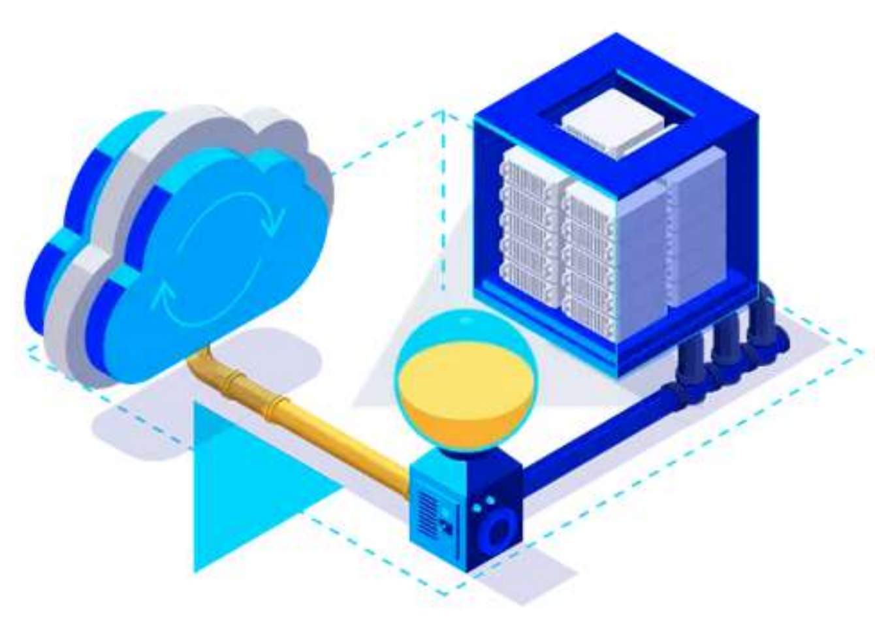
- **Vérifiez** les services de sauvegarde intégrés aux solutions que vous utilisez.
- **Orientez-vous** vers des solutions de stockage standards, sécurisées et adaptées à vos besoins (conformité, performances, prix, etc.) présents et à venir.
- **Pensez** également à la réplication de vos données (copie et stockage à plusieurs endroits) dans le but d'en améliorer la disponibilité et l'accessibilité.

Côté fournisseur

Avant de faire votre choix, nous vous conseillons de détailler l'ensemble des garanties proposées : conformité, souveraineté, engagements de niveaux de service SLA, réversibilité, etc.

OVHcloud

C'est plus de 20 ans d'expertise



- **Des infrastructures hautement résilientes,** certifiées et sécurisées qui hébergent des services intégrés et interopérables.
- **Des factures prévisibles,** sans frais cachés, pour vous permettre de contrôler précisément vos investissements.
- **Un écosystème de spécialistes,** composé des principaux acteurs de la protection des données (NetApp, Nutanix, Veeam, VMware et Zerto) ainsi qu'un réseau de plus de 1 000 partenaires.

Sources :

[1] Selon *Moore's Law*, une observation empirique faite par le cofondateur d'Intel, corroborée par de nombreux rapports de recherche et études publiés notamment par le cabinet d'analyse IDC et EMC Corporation

[2] Selon une estimation extraite du livre blanc intitulé *The State of Ransomware and Disaster Preparedness* réalisé par IDC et publié en mai 2022

[3] Selon une estimation extraite de l'étude intitulée *Cost of a Data Breach Report* réalisée par IBM en 2020

[4] Selon le rapport annuel intitulé *intitulé The Cost of a Data Breach Report 2021 basé sur la l'analyse des données d'IBM Security et compilé par Ponemon Institute*

[5] Selon le rapport annuel intitulé *2021 SonicWall Cyber Threat Report*

Infographie réalisée en juin 2023