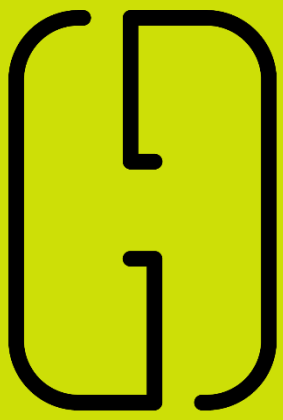


GROUPEHISI

Faire face aux cyber-attaques et sécuriser les données vitales

Sommaire

- Les enjeux de la sauvegarde
- Sécuriser la donnée, patrimoine de l'entreprise
- Le statut de la sauvegarde évolue
- La sauvegarde : une protection en cas de cyber-attaques
- Conclusion

Les enjeux de la sauvegarde

La protection de la donnée : votre application critique N°1 ?

Dans le contexte de la croissance exponentielle des données, de leur valorisation et des risques liés aux cyber-attaques, maîtriser ses sauvegardes s'applique:

- Pour tout domaine d'activité
- Pour tout outil de sauvegarde
- En fonction de l'externalisation souhaitée : duplication de 1 à n copies avec un niveau de sécurité dès la conception de la plateforme.

Dans le passé, la sauvegarde faisait partie de l'infrastructure., les moyens mis en œuvre permettaient souvent un souvent un recouvrement de données pour des besoins locaux ou ponctuels ou pour limiter un Incident mineur sur un fichier, un serveur …

Nombreux furent les cas où les sauvegardes ne permettaient pas de recouvrer toutes les données dans un incident majeur, de très grande ampleur (incendie, cyberattaques, malveillance…) Et pour les organisations les mieux loties, la récupération des données était liée à de grands efforts et sur un temps de traitement important !

COMPLEXITÉ

Aujourd'hui, les environnements technologiques sont de plus en plus complexes et imposent l'imbrication de différentes couches techniques. Les sauvegardes s'appliquent donc à différents niveaux : OS, VM, Applications …

DONNÉES

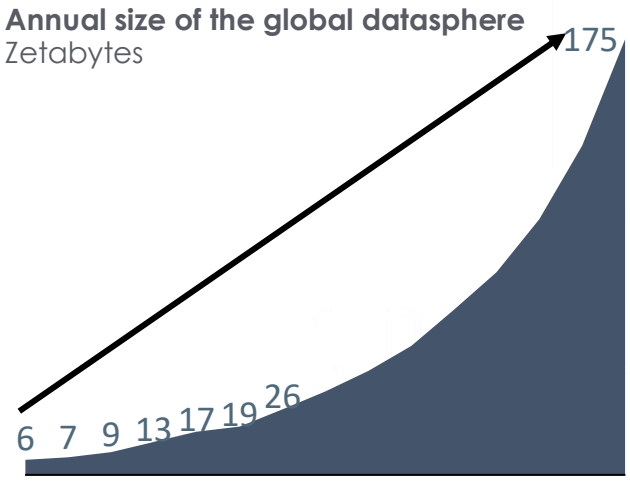
Dans une ère de l'immédiateté, d'un « time to market » réduit et de l'importance vitale des données, les équipes IT subissent une forte pression liée à l'attente des directions, des clients, et utilisateurs.

MENACES

Les menaces amènent également les directions générales à augmenter leurs exigences en matière de restauration et sécurisation de la donnée. Il n'est pas rare d'être confronté à une erreur humaine souvent conséquence de la complexité technologique des plateformes. Les attaques liées à la cybercriminalité ou les risques de malveillance augmentent de manière drastique depuis un an. L'ANSSI a noté une augmentation de **255%** des signalements d'attaque par rançongiciel dans son périmètre en 2020 par rapport à 2019. Les impacts directs (perte d'activité, de CA, d'argent) et indirects (image, notoriété, motivation des équipes) dépassent largement le budget d'une architecture de sauvegarde qu'on peut qualifier « d'optimale »

Sécuriser la donnée, patrimoine de l'entreprise

Plus on crée de la donnée, moins on la maîtrise



175 ZB en 2025
1 ZB = 1,000,000 PB

55% dark data

Responsabilité partagée: le mode SaaS implique une sauvegarde dédiée

Responsabilité du Cloud Provider
Infrastructure, application, et disponibilité du service

Responsabilité du Client
Protéger ses propres données

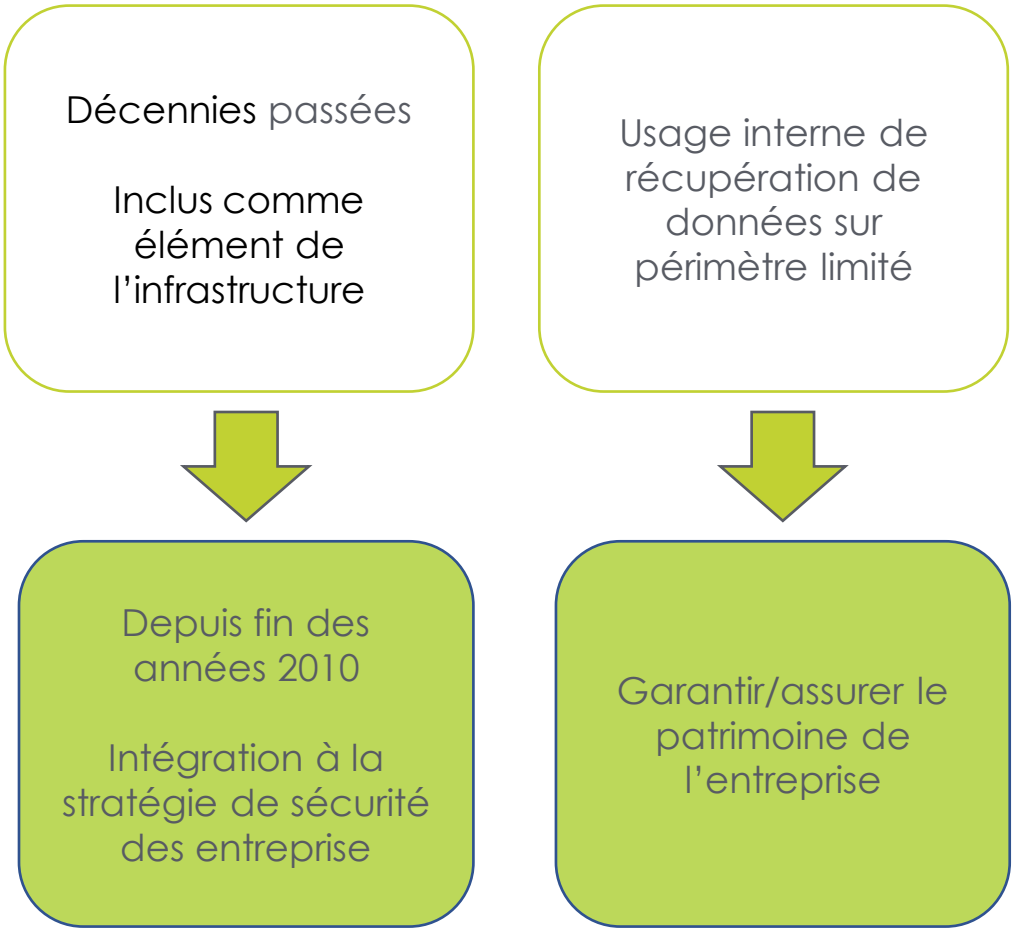
Les données doivent être protégés quelque soit le modèle : infrastructure On Premise, Cloud Public IaaS, PaaS sans oublier le SaaS ! Parce que les application sont en SaaS, l'équipe IT n'a pas à se soucier des menaces traditionnelles comme les pannes de serveur ou de stockage, les inondations ou les incendies dans le datacenter, etc.

Cependant, l'entreprise ou organisation cliente du fournisseur SaaS reste toujours responsable de ses données et de ce qui peut leurs arriver (Ransomware, malware, suppression accidentelle, malveillance). La protection des données devient partie intégrante de la sécurité de bout en bout, il faut pouvoir parer tout incident ou perte de données.

Le statut de la sauvegarde évolue

Autrefois élément mineur de l'infrastructure, la sauvegarde est devenue une composante à part entière de la stratégie de sécurité globale des entreprises. Les enjeux de sécurisation de la donnée et l'accroissance des cyber-attaques (vol de données) ont fait évoluer la sauvegarde vers un statut intégrant :

- La prise en compte des usages, des nouvelles technologies
- L'évolution dans le Cloud qui impose de protéger ses données et de s'assurer de leur localisation
- La protection face aux attaques : la capacité de pouvoir repartir sur des données fiables même en cas d'attaque grâce aux sauvegardes
- Une sauvegarde non disruptive
- Des fonctionnalités avancées permettant de gérer la granularité des sauvegardes.



La sauvegarde : une protection en cas de cyber-attaque

Une stratégie complète de protection contre les ransomwares comprend à la fois la réduction du risque d'une attaque aboutie et l'atténuation de l'impact de cette attaque. Les cinq étapes pour se protéger sont : **planifier, prévenir, surveiller, restaurer (rapidement) et tester.**

Un plan efficace est le fondement d'une reprise complète et rapide des activités normales. Prévenir les attaques via des actions proactives incluant les couches techniques dites « basses », les applications et la protection contre les ransomwares. Surveiller l'environnement en étant constamment à l'affût de toute anomalie, détecter l'attaque le plus rapidement possible pour en réduire l'impact. Restaurer les données grâce à des restaurations rapides avec une copie de données intacte pour reprendre rapidement les activités commerciales et réduire l'impact des ransomwares.

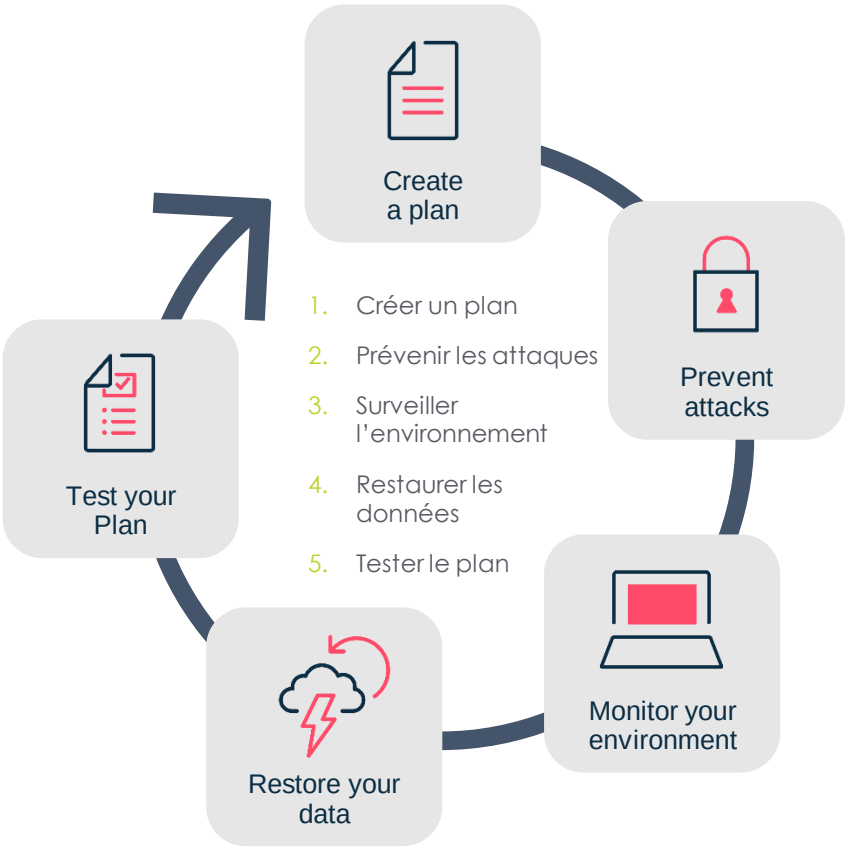
Identifier	Identifier et atténuer les risques pesant sur les données de sauvegarde au sein d'une unique interface
Protéger	Appliquer des contrôles de sécurité basés sur les normes de référence du secteur : Sauvegardes immuables
Surveiller	Alerter et surveiller la présence de ransomware, de menaces internes et d'autres menaces.
Agir	Agir sur les menaces et valider en permanence l'intégrité des données de sauvegarde
Sécuriser	Infrastructure de sauvegarde résiliente

Tester pour sécuriser

* Forrester, The State Of Disaster Recovery Preparedness In 2020 Review Business And IT Risks With Evolving Business Operations by Naveen Chhabra August 24, 2020.

Point crucial, il faut tester son plan en effectuant des tests fréquents pour vérifier le respect des SLA définis pour les données et les applications hautement prioritaires, que la sauvegarde soit gérée par le service IT interne ou par un prestataire de services externe.

Les tests permettent de vérifier que le personnel et les ressources connaissent les processus et les maîtrisent. Ils permettent de valider l'intégrité des données et des copies de sauvegarde, de vérifier que les données, les applications et les systèmes sont prêts à être restaurés, identifier et corriger toute insuffisance des niveaux de service, réviser et mettre à jour le plan de reprise après sinistre si nécessaire,



La sauvegarde préambule du PRI ou Disaster Recovery

La sauvegarde permet de restaurer rapidement des données et favorise une reprise rapide des opérations. La sécurisation des sauvegardes est un préambule au PRI ou Disaster Recovery.

Backup and recovery

Disponibilité des données pour toutes les charges de travail dans les environnements en cloud et On-premise.

Disaster recovery

Réduire au minimum les interruptions d'activité et répondre aux besoins de continuité des activités.

Protection Ransomware

Approche de sécurité multicouche pour gérer le risque de ransomware et garantir la disponibilité des données..

Faire soi-même ou faire faire ?

Externaliser le service permet de s'affranchir des contraintes liées à la sauvegarde :

- Suivi et évolution de l'espace de stockage, résilience de la donnée, protection de la donnée
- Déléguer les tâches d'administration basique ou même avancée, répétitives et chronophages
- Disposer d'une plateforme avec SLA garantis et dotée d'un reporting avancé

Externaliser la sauvegarde des données est gage de sécurité, encore faut-il vérifier où les données sont stockées dans un contexte réglementaire contraignant (souveraineté, RGPD) et comment elles sont gérée par le prestataire externe.

Les avantages de l'externalisation de la sauvegarde :

- ❑ Pas d'investissement OPEX
- ❑ Une infogérance globale
- ❑ Flexibilité et évolutivité
- ❑ Reporting avancé pour la DSI, la Direction Générale et les métiers