

Sauvegarder Microsoft 365 / Google Workspace : oui, c'est nécessaire

« C'est dans le cloud, c'est sauvegardé » — non. Ce que les suites protègent vraiment, ce qu'elles ne protègent pas, et comment combler le trou.

7 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/sauvegarde-microsoft-365

L'idée reçue la plus coûteuse du cloud : « Microsoft/Google sauvegarde nos données ». En réalité, les suites garantissent leur infrastructure (vos données ne disparaîtront pas par panne de leurs serveurs) — mais VOS suppressions, VOS comptes piratés, VOS ransomwares synchronisés restent votre problème, avec des filets natifs limités à quelques semaines. C'est le modèle de responsabilité partagée, écrit noir sur blanc dans les contrats. Le trou se comble simplement — encore faut-il savoir qu'il existe.

1. Ce que les suites protègent — et ne protègent pas

- Protégé : la panne de LEUR infrastructure — réplication multi-datacenters, votre donnée survit à leurs incidents matériels
- Filets limités : corbeilles (30-90 jours selon les cas), historique de versions, rétentions par défaut — utiles pour l'erreur d'hier, pas pour celle découverte dans trois mois
- Pas protégé : la suppression (accidentelle ou malveillante) au-delà des rétentions, le compte administrateur compromis qui purge, le ransomware qui chiffre via la synchronisation, le compte supprimé dont on redécouvre le besoin, l'application tierce qui corrompt
- Écrit dans les contrats : Microsoft comme Google recommandent explicitement la sauvegarde tierce de vos contenus — la responsabilité des données vous reste

CAS CONCRET

Le scénario vécu qui convertit les sceptiques : un litige prud'homal exige les échanges d'un salarié parti 8 mois plus tôt — compte supprimé après le délai standard de rétention, boîte irrécupérable. Ou : un ransomware chiffre les fichiers d'un poste, OneDrive synchronise consciencieusement les versions chiffrées, et la restauration en masse via l'historique natif tourne au chemin de croix. La sauvegarde tierce règle les deux en quelques clics.

2. La sauvegarde tierce : quoi couvrir

- Les boîtes email (et leurs archives), les agendas et contacts
- OneDrive/Drive de chaque utilisateur ET les espaces partagés (SharePoint, Drive partagés) — souvent oubliés
- Teams/Chat selon les besoins de conservation
- Le périmètre suit vos obligations d'archivage : ce qui doit être conservable 5-10 ans ne peut pas dépendre d'une corbeille de 30 jours

3. Choisir et mettre en place

- Les solutions dédiées (nombreuses et matures) se branchent en 30 minutes via les API des suites : sauvegarde automatique quotidienne, rétention illimitée ou longue, restauration granulaire (UN email, UN fichier, UNE boîte entière)
- Les critères : couverture complète (partagés inclus !), localisation des données (UE), rétention adaptée à vos durées légales, simplicité de restauration testée
- Le stockage de la sauvegarde HORS de la suite sauvegardée : une sauvegarde 365 stockée... dans 365 rate l'objectif
- Budget : quelques euros par utilisateur et par mois — à comparer au coût d'une boîte irrécupérable
- Souvent inclus ou proposé par votre prestataire d'infogérance : posez la question explicitement

4. Compléter par les réglages natifs

- Allonger les rétentions natives là où les licences le permettent (stratégies de rétention) : le premier filet gratuit
- Verrouiller les suppressions définitives : qui peut purger quoi, avec quelles alertes
- Protéger les comptes admin (MFA maximale) : la sauvegarde tierce protège aussi de leur compromission — à condition que l'attaquant ne puisse pas la couper aussi (compte de sauvegarde séparé et durci)
- Tester la restauration une fois par trimestre : un email précis d'il y a 6 mois, un dossier partagé — le rituel standard s'applique au cloud comme au reste

L'essentiel à retenir

- 01 Acter que la suite ne sauvegarde pas au sens de vos besoins
- 02 Déployer une sauvegarde tierce : boîtes, drives, espaces partagés
- 03 Stocker la sauvegarde hors de la suite, en UE, rétention légale
- 04 Durcir le compte de sauvegarde lui-même (MFA, accès séparé)
- 05 Allonger les rétentions natives en complément
- 06 Tester une restauration granulaire chaque trimestre

Questions fréquentes

Nous avons l'historique de versions et la corbeille. Pourquoi payer en plus ?

Pour les trois scénarios qu'ils ne couvrent pas : la découverte tardive (le fichier écrasé il y a 4 mois, la boîte du salarié parti l'an dernier), la restauration en masse après incident (des milliers de fichiers via l'interface de versions = des jours), et la malveillance avec droits (l'admin compromis purge corbeilles ET versions). La sauvegarde tierce coûte le prix d'un café par utilisateur — c'est l'assurance du cloud.

Où est stockée la sauvegarde tierce, et est-ce RGPD-compatible ?

Chez l'éditeur de sauvegarde ou sur le stockage que vous désignez — exigez l'option datacenters UE et le DPA (article 28) comme pour tout sous-traitant. Paradoxalement, la sauvegarde AMÉLIORE votre conformité : capacité à restaurer (intégrité), à retrouver (droits d'accès), et à purger selon vos durées si l'outil gère les rétentions.

Et les autres SaaS (CRM, facturation, compta en ligne) ?

Même logique, réponse variable : vérifiez pour chacun ce que le fournisseur garantit, ce que vous pouvez exporter, et automatisez un export régulier des données critiques (la plupart des outils sérieux ont exports ou API). Le réflexe à systématiser au choix de tout SaaS : « comment récupère-t-on nos données, et qui les sauvegarde ? » (voir notre guide).

Pour aller plus loin

Microsoft — modèle de responsabilité partagée — learn.microsoft.com/fr-fr/compliance/assurance/assurance-shared-responsibility

Cybermalveillance.gouv.fr — les sauvegardes — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

Vos sauvegardes tiendraient-elles le choc ?

Mise en place, tests de restauration, plan de reprise : nous rendons votre activité résiliente, à votre échelle.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr