

Checklist : 15 signaux d'alerte que vos données M365 sont à risque

Votre environnement Microsoft 365 est-il vraiment sous contrôle ? Un diagnostic simple pour identifier rapidement vos zones d'exposition.

80% des violations de données impliquent aujourd'hui des environnements collaboratifs (emails, Teams, OneDrive, SharePoint).

Et pourtant, une part importante des accès et des partages restent peu ou mal suivis dans le temps.

Cette checklist vous permet :

- d'identifier rapidement les situations à risque
- de comprendre quelles données sensibles sont exposées
- de savoir par où commencer

Si vous cochez **5 signaux ou plus**, votre exposition mérite une analyse prioritaire.



Partages & accès

→ 1. Des liens de partage anonymes sont actifs

Risque : accès non traçable à des données sensibles

Action : désactiver ou limiter les liens anonymes

→ 2. Des utilisateurs externes ont encore accès à des espaces anciens

Risque : accès persistant après fin de collaboration

Action : auditer et supprimer les invités inactifs

→ **3. Des données sensibles sont accessibles à un grand nombre d'utilisateurs**

Risque : exposition involontaire

Action : appliquer le principe du moindre privilège

→ **4. Des documents sont partagés à l'externe sans validation préalable**

Risque : diffusion non maîtrisée de contenus sensibles

Action : mettre en place un processus de validation



Droits & revue des accès

→ **5. Certains espaces n'ont pas de propriétaire clairement identifié**

Risque : absence de responsabilité sur les accès

Action : nommer un owner + un backup

→ **6. Des accès accordés pour un besoin ponctuel sont encore actifs plusieurs mois après**

Risque : accumulation silencieuse de permissions devenues inutiles

Action : mettre en place des campagnes de revue régulières

→ **7. Les propriétaires de données n'ont pas de visibilité sur les accès qu'ils accordent dans le temps**

Risque : décalage entre les usages réels et les droits maintenus

Action : impliquer les métiers dans la revue périodique des accès

→ **8. Les règles de partage sont définies mais peu appliquées dans les usages quotidiens**

Risque : écart entre gouvernance théorique et pratiques réelles

Action : revalider les partages actifs selon des règles simples



Visibilité & pilotage

→ **9. Vous ne savez pas où se trouvent les données les plus sensibles**

Risque : priorisation impossible

Action : identifier et classer les données critiques

→ 10. Vous n'avez pas de vision globale de qui accède à quoi

Risque : angles morts importants

Action : cartographier les accès et les partages réels

→ 11. Vous n'avez pas de vision sur les invités et les prestataires externes

Risque : des comptes avec des privilèges parfois excessifs

Action : identifier et gérer les permissions et groupes M365 liés aux externes (Entra ID Guest B2B + SharePoint Guests)



Usages & dynamique

→ 12. Les espaces Teams / SharePoint sont créés facilement, mais rarement nettoyés ou archivés

Risque : explosion de la surface d'exposition

Action : encadrer le cycle de vie des espaces

→ 13. Les utilisateurs ne voient pas clairement les accès qu'ils ont accordés

Risque : multiplication d'accès non maîtrisés, surtout en cas d'invités externes

Action : proposer un bilan de santé des données pour chaque utilisateur



IA & Nouveaux risques

→ 14. Vos données sont accessibles à des outils d'IA sans contrôle précis

Risque : amplification de l'exposition

Action : encadrer les usages via des politiques claires et responsabiliser les métiers

→ 15. Vous ne savez pas quelles données peuvent être exploitées par l'IA

Risque : perte de maîtrise

Action : identifier les données critiques et leur exposition

INTERPRÉTATION

0 à 3 signaux

Situation globalement maîtrisée (à surveiller)

Continuez à suivre vos accès et partages dans le temps pour éviter toute dérive. Besoin d'un point de contrôle rapide ?

Demander un diagnostic flash

4 à 7 signaux

Exposition réelle à traiter en priorité

Certains accès et partages présentent déjà un risque. Identifiez précisément les zones à corriger.

Évaluer votre environnement M365

8 signaux ou plus

Risque élevé, votre environnement nécessite une action rapide

Vos données sont probablement exposées à des accès non maîtrisés. Priorisez les actions critiques avec un diagnostic structuré.

Demander un diagnostic prioritaire

Vous souhaitez évaluer votre exposition réelle ?

Identifiez rapidement :

- ✓ Les accès à risque
- ✓ Les zones critiques
- ✓ Les partages sensibles

Demandez un diagnostic !