

Sécuriser Microsoft 365 / Google Workspace

Votre messagerie et vos fichiers vivent dans le cloud — leur sécurité dépend de dix réglages que peu d'entreprises activent.

11 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/securiser-microsoft-365

Microsoft 365 et Google Workspace concentrent l'essentiel de la vie numérique de l'entreprise : emails, fichiers, agendas, visio. Les plateformes sont solides — mais livrées avec des réglages pensés pour la simplicité, pas pour la sécurité. La quasi-totalité des comptes piratés le sont via des configurations par défaut jamais durcies. Voici le tour du propriétaire, valable pour les deux écosystèmes.

1. Identités : le chantier n° 1

- MFA obligatoire pour TOUS les utilisateurs — pas seulement les admins ; les deux plateformes le proposent nativement (chez Microsoft, les « security defaults » ou l'accès conditionnel l'imposent)
- Comptes administrateurs dédiés, séparés du compte de travail quotidien, protégés au niveau maximal (clé physique idéalement), et au nombre de deux ou trois maximum
- Bloquer l'« authentification héritée » (protocoles anciens qui contournent la MFA) — le trou classique des locataires Microsoft anciens
- Examiner les connexions à risque : les deux consoles signalent les connexions depuis des pays ou appareils inhabituels

ATTENTION

Le compte administrateur global avec le même mot de passe depuis 2019, sans MFA, utilisé au quotidien pour lire ses emails : c'est le jackpot de l'attaquant — il contrôle alors messagerie, fichiers et règles de TOUTE l'entreprise. Les comptes admin se séparent, se protègent au maximum et ne servent qu'à administrer.

2. Messagerie : fermer les portes dérobées

- Auditer les règles de transfert automatique vers l'extérieur — l'outil favori des attaquants pour lire votre courrier en silence après compromission ; les bloquer par défaut
- Activer les protections anti-phishing avancées incluses dans votre licence (Defender pour Office 365 / protections Gmail) : liens vérifiés au clic, pièces jointes détonnées en bac à sable
- Configurer SPF, DKIM et DMARC sur votre domaine (voir notre guide dédié)
- Alerter sur les actions sensibles : création de règles de boîte, connexions admin, suppressions massives

3. Partage de fichiers : reprendre le contrôle

- Régler le partage par défaut : « personnes spécifiques » plutôt que « toute personne disposant du lien »
- Faire expirer les liens de partage externes et revoir périodiquement ce qui est partagé hors de l'entreprise
- Encadrer les partages « Tout le monde dans l'organisation » : le dossier paie partagé à toute l'entreprise est un classique d'audit

- Limiter ou surveiller la synchronisation sur appareils personnels non gérés

4. Applications tierces : le shadow IT du cloud

« Se connecter avec Microsoft/Google » est pratique — et chaque autorisation accorde à une application tierce un accès durable à des données de l'entreprise, parfois la lecture complète de la messagerie. Les attaquants exploitent ce mécanisme avec de fausses applications (consent phishing).

- Passer en revue les applications autorisées dans la console d'administration — il y a toujours des surprises
- Restreindre le consentement : les demandes d'accès sensibles passent par validation d'un administrateur
- Révoquer ce qui ne sert plus ou qu'on ne reconnaît pas

5. Sauvegarder — oui, même le cloud

Corbeilles et rétentions intégrées protègent quelques semaines, pas plus : une suppression malveillante, un compte piraté qui vide les boîtes, un ransomware qui chiffre via la synchronisation — et les données partent aussi des « sauvegardes » natives. Pour les données critiques, une sauvegarde tierce dédiée à Microsoft 365 / Workspace (emails, drives, sites) est le filet que les plateformes elles-mêmes recommandent. Complétez avec les scores de sécurité intégrés (Microsoft Secure Score, tableau de bord sécurité Google) : ils listent vos manques, priorisés — un audit gratuit permanent.

L'essentiel à retenir

- 01 Imposer la MFA à tous les utilisateurs, bloquer l'authentification héritée
- 02 Séparer et surprotéger les comptes administrateurs
- 03 Bloquer les transferts automatiques vers l'extérieur, auditer les règles de boîte
- 04 Régler le partage de fichiers par défaut sur « personnes spécifiques »
- 05 Passer en revue les applications tierces autorisées
- 06 Mettre en place une sauvegarde tierce des données critiques
- 07 Suivre le score de sécurité de la plateforme et traiter ses recommandations

Questions fréquentes

Ces protections nécessitent-elles des licences plus chères ?

L'essentiel — MFA, blocage de l'authentification héritée, règles de partage, revue des applications, alertes de base — est inclus dans toutes les licences professionnelles. Les licences supérieures ajoutent l'accès conditionnel fin, la détonation des pièces jointes ou la prévention de fuite de données : utiles, mais commencez par activer ce que vous payez déjà — la marge de progression y est énorme.

Un compte utilisateur 365 a été piraté : les bons gestes ?

Dans l'ordre : réinitialiser le mot de passe ET révoquer toutes les sessions actives ; vérifier et supprimer les règles de boîte créées (transferts, suppressions automatiques) ; vérifier les applications tierces récemment autorisées et les appareils enregistrés pour la MFA ; examiner les traces (emails envoyés, fichiers touchés) pour évaluer les dégâts ; puis chercher comment l'attaquant est entré — souvent un phishing, parfois l'authentification héritée.

Qui doit faire ce durcissement : nous ou un prestataire ?

Un administrateur soigneux fait beaucoup avec les scores de sécurité intégrés comme fil rouge. Le passage par un prestataire se justifie pour l'accès conditionnel, la migration sans casse de l'existant (bloquer l'authentification héritée peut couper un vieux copieur qui scanne vers email) et la surveillance continue. Bon compromis fréquent : un durcissement initial professionnel, puis une revue annuelle.

Pour aller plus loin

Microsoft — Secure Score et bonnes pratiques 365 — learn.microsoft.com/fr-fr/defender-office-365/step-by-step-guides/secure-by-default

Google — check-list sécurité Workspace — support.google.com/a/answer/9184226

ANSSI — Guide d'hygiène informatique — cyber.gouv.fr/publications/guide-dhygiene-informatique

Un projet cloud ou d'infrastructure ?

Choix, migration, sécurisation, supervision : Cyberionis conçoit des infrastructures sobres et qui durent.
contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr