

GUIDE

Durcir Microsoft 365 & Google Workspace, pas à pas

Six gestes concrets pour transformer votre suite collaborative en forteresse : MFA anti-phishing, comptes admin dédiés, accès conditionnel, audit et coupure des protocoles hérités.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~12 min Édition 2026 sedona-ai.com

Durcir Microsoft 365 et Google Workspace tient en six gestes que votre administrateur peut poser en une journée : activer un MFA résistant au phishing, isoler les comptes admin, appliquer un accès conditionnel, couper l'authentification héritée, cadrer le partage externe et activer l'audit. Selon Microsoft, le seul MFA bloque déjà plus de 99,9 % des tentatives de compromission de compte. Ce tutoriel vous guide écran par écran, sur les deux plateformes, du minimum gratuit jusqu'aux réglages avancés.

À retenir

- Le MFA est la mesure la plus rentable : selon Microsoft, il bloque plus de 99,9 % des tentatives de compromission de compte.
- Privilégiez un MFA résistant au phishing (passkeys, clés FIDO2), lié cryptographiquement au domaine — un OTP par SMS reste interceptable par un site usurpé.
- Distinguez le gratuit du payant : les security defaults Entra ID couvrent le minimum ; l'accès conditionnel granulaire exige une licence Entra ID P1/P2, et le Context-Aware Access de Google une édition Enterprise.
- Coupez l'authentification héritée (Basic Auth) : elle transmet les identifiants en clair et ignore le MFA — c'est le vecteur que Microsoft cite pour son retrait d'Exchange Online.
- Vérifiez la rétention de vos journaux d'audit avant de promettre une investigation rétroactive : 180 jours par défaut hors E5, 1 an avec E5 sur M365.
- Appuyez-vous sur des référentiels publics et gratuits : guide ANSSI-PG-078 (aligné RGPD art. 5 et 32) et CIS Foundations Benchmarks M365 / Google Workspace.

01 Le MFA, premier rempart (et le plus rentable)

Avant tout réglage avancé, une seule mesure change la donne : l'authentification multifacteur. Un mot de passe volé ne suffit plus à ouvrir une boîte mail si un second facteur protège le compte. Les chiffres de Microsoft, tirés de l'observation de ses propres services cloud, sont sans appel.

99,9 %

des tentatives de compromission de compte bloquées par le seul MFA, selon Microsoft
Microsoft Security Blog, 2019

300 M/jour

de tentatives de connexion frauduleuses observées par Microsoft sur ses services cloud
Microsoft Security Blog, 2019

À lire comme « selon Microsoft »

Ce chiffre de 99,9 % provient d'une étude interne Microsoft de 2019 sur ses comptes cloud, pas d'une mesure académique indépendante. Il reste néanmoins l'ordre de grandeur de référence dans l'industrie : le MFA n'est pas une option, c'est le socle.

02 Étape 1 — Déployer un MFA résistant au phishing

Tous les MFA ne se valent pas. Un code par SMS ou une application d'authentification (OTP) peut être capté par un site d'hameçonnage qui vous relaie en temps réel. Les passkeys et les clés de sécurité FIDO2 sont, elles, liées cryptographiquement au vrai domaine : elles refusent de s'authentifier sur un site usurpé. Visez ce niveau pour les comptes sensibles, à commencer par les administrateurs.

1 Microsoft 365 — activer le socle gratuit

Dans le centre d'administration Microsoft Entra : Identité > Vue d'ensemble > Propriétés > Gérer les valeurs de sécurité par défaut (security defaults). Cela impose le MFA à tous les utilisateurs et bloque l'authentification héritée, sans licence payante.

2 Microsoft 365 — activer FIDO2 / passkeys

Entra > Protection > Méthodes d'authentification : activez « Passkey (FIDO2) » et « Microsoft Authenticator ». Enregistrez au moins une clé physique par compte administrateur comme facteur de secours anti-phishing.

3 Google Workspace — imposer la validation en 2 étapes

Console d'admin > Sécurité > Authentification > Validation en 2 étapes : activez l'application, puis pour les comptes sensibles choisissez l'option « Clé de sécurité uniquement » — qui accepte désormais aussi bien les clés physiques que les passkeys, avec le même niveau de protection contre le phishing.

Commencez par les comptes à haut risque

Déployez les clés FIDO2 / passkeys d'abord sur les administrateurs, la direction et la finance. Ce sont les cibles prioritaires du phishing et de la fraude au président.

03 Étape 2 — Isoler les comptes d'administration

Un administrateur qui lit ses mails et navigue avec son compte à privilèges expose l'ensemble du tenant au premier lien piégé. La règle : un compte d'admin dédié, sans boîte mail courante, réservé aux tâches d'administration.

1. Créez un compte admin distinct par personne (jamais de compte partagé), nommé sans ambiguïté (ex. admin-prenom).
2. Retirez les licences superflues : le compte admin n'a pas besoin d'Exchange, Teams ou Drive pour administrer.
3. Protégez-le par une clé FIDO2 / passkey obligatoire, sans exception ni contournement.

4. Appliquez le moindre privilège : attribuez des rôles ciblés plutôt que « Administrateur général » à tout le monde, et limitez le nombre de comptes disposant des droits les plus élevés.
5. Conservez au moins un compte d'accès d'urgence (« break-glass ») documenté et surveillé, exclu des règles qui pourraient vous verrouiller dehors.

04 Étape 3 — Poser un accès conditionnel

L'accès conditionnel décide qui peut se connecter, depuis où et dans quelles conditions : exiger le MFA hors du réseau de l'entreprise, bloquer les pays sans activité, imposer un appareil conforme. C'est la couche qui adapte la sécurité au risque réel de chaque connexion.

- 1 Microsoft 365 (licence P1/P2)**
Entra > Protection > Accès conditionnel : créez une politique exigeant le MFA pour tous, une seconde bloquant l'authentification héritée, une troisième renforçant les administrateurs. Ciblez une exclusion pour le compte break-glass.
- 2 Google Workspace (édition Enterprise)**
Console d'admin > Sécurité > Context-Aware Access : définissez des niveaux d'accès (ex. exiger la 2SV hors réseau d'entreprise) et appliquez-les aux applications — y compris à la console d'administration elle-même.

Ne confondez pas gratuit et payant

Sur Microsoft 365, l'accès conditionnel granulaire nécessite une licence Entra ID P1 ou P2 ; il n'est pas compatible avec les security defaults activés simultanément sur le même tenant (choisissez l'un ou l'autre). Côté Google, le Context-Aware Access est réservé aux éditions Enterprise. Sans ces licences, tenez-vous-en au socle gratuit décrit à l'étape 1.

05 Étape 4 — Couper l'authentification héritée

Les vieux protocoles (POP, IMAP, EWS, SMTP AUTH...) utilisant le Basic Auth transmettent les identifiants en clair et ne savent pas gérer le MFA. C'est précisément pour cela que Microsoft a retiré le Basic Auth des principaux protocoles Exchange Online en octobre 2022. Tant qu'ils restent ouverts, votre MFA a une porte dérobée.

SMTP AUTH : vérifiez le calendrier à jour

Le SMTP AUTH Client Submission a fait exception : d'après Microsoft, il reste inchangé jusqu'à fin décembre 2026, puis sera désactivé par défaut pour les tenants existants (réactivable par l'admin), et indisponible par défaut pour les nouveaux tenants (OAuth uniquement). Ce calendrier a déjà été repoussé plusieurs fois — confirmez la date en vigueur sur Microsoft Learn avant d'agir.

- 1 Microsoft 365**
Les security defaults et l'accès conditionnel bloquent l'authentification héritée. Recensez les usages légitimes restants (imprimantes, scripts d'envoi) et migrez-les vers OAuth 2.0 avant de couper.

2 Google Workspace

Console d'admin > Sécurité > Contrôle des accès et des données > Applications moins sécurisées : désactivez l'accès pour tous les utilisateurs afin d'interdire les connexions par mot de passe seul sur des clients obsolètes.

06 Étape 5 — Maîtriser le partage externe

Un dossier partagé « à toute personne disposant du lien » est une fuite de données qui s'ignore. L'objectif n'est pas d'interdire le partage, mais de le rendre traçable et limité dans le temps.

1 Microsoft 365 (SharePoint / OneDrive)

Centre d'administration SharePoint > Partage : passez le niveau par défaut sur « Personnes nouvelles et existantes » plutôt que « N'importe qui », activez l'expiration des liens invités et le domaine de destinataires autorisés.

2 Google Workspace (Drive)

Console d'admin > Applications > Google Workspace > Drive et Docs > Partage : restreignez le partage hors du domaine, désactivez le partage vers des liens publics par défaut et activez les avertissements lors d'un partage externe.

3 Revue périodique

Planifiez un audit trimestriel des partages externes actifs et révoquez les liens dormants — un partage utile un jour devient un risque oublié.

07 Étape 6 — Activer la journalisation et l'audit

Sans journaux, une compromission reste invisible et impossible à instruire. Les deux plateformes journalisent les connexions, les changements de configuration et les accès aux fichiers — encore faut-il l'activer et connaître la durée de conservation.

La rétention dépend de votre licence

Sur Microsoft 365, le Purview Unified Audit Log (Entra ID, Exchange, SharePoint, Teams...) conserve les enregistrements 180 jours par défaut hors E5, et 1 an par défaut avec une licence E5 (ou l'add-on eDiscovery & Audit), extensible jusqu'à 10 ans via un add-on dédié. Vérifiez ce point avant de promettre une capacité d'investigation rétroactive.

- ☐ M365 : confirmer que l'audit unifié Purview est activé et connu de l'équipe (portail Microsoft Purview > Audit).
- ☐ Google Workspace : consulter et exporter les journaux d'audit (Console d'admin > Reporting > Audit et investigation).
- ☐ Router les journaux vers un stockage ou un SIEM externe si la rétention native ne couvre pas vos obligations.

08 Vérifier votre surface et s'appuyer sur les référentiels

Le durcissement interne se double d'un regard extérieur : que voit un attaquant de votre organisation ? Domaines, sous-domaines, services exposés, e-mails divulgués. C'est le point de départ d'un ciblage — et donc de votre défense.

- Guide ANSSI-PG-078 « authentification multifacteur et mots de passe » : référence gratuite, élaborée avec la CNIL et positionnée comme appui pour la conformité RGPD (articles 5 et 32), qui place le MFA parmi les mesures prioritaires.
- CIS Microsoft 365 Foundations Benchmark et CIS Google Workspace Foundations Benchmark : listes de contrôle détaillées, téléchargeables gratuitement en PDF (usage non commercial), à confronter à votre configuration.
- Une revue régulière de votre surface d'attaque externe pour repérer ce qui a été exposé par erreur ou oublié.

Radar évalue, il ne certifie pas

Sedona Radar analyse ce que votre domaine expose sur Internet et donne des indicateurs de maturité face à des référentiels comme NIS2 ou l'Hygiène ANSSI. C'est une aide à la décision : Radar ne certifie rien, et il n'existe aucune certification NIS2. Radar ne voit pas la configuration interne de votre locataire Microsoft 365 ou Google Workspace.

§ Sources

1. Microsoft Security Blog — One simple action you can take to prevent 99.9 percent of attacks on your accounts (2019) — <https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>
2. Microsoft Learn — Deprecation of Basic authentication in Exchange Online — <https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>
3. Microsoft Learn — Configure Security Defaults for Microsoft Entra ID — <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>
4. Microsoft Learn — Manage audit log retention policies (Purview) — <https://learn.microsoft.com/en-us/purview/audit-log-retention-policies>
5. Google Workspace Admin Help — Deploy 2-Step Verification — <https://knowledge.workspace.google.com/admin/security/deploy-2-step-verification>
6. Google Workspace Admin Help — Assign Context-Aware access levels to the Admin console — <https://knowledge.workspace.google.com/admin/security/assign-context-aware-access-levels-to-the-admin-console>
7. ANSSI / MesServicesCyber — Guide authentification multifacteur et mots de passe (ANSSI-PG-078) — https://mes-services.cyber.gouv.fr/documents-guides/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf
8. CIS — CIS Microsoft 365 Foundations Benchmark — https://www.cisecurity.org/benchmark/microsoft_365
9. CIS — CIS Benchmarks (portail général, inclut Google Workspace Foundations) — <https://www.cisecurity.org/cis-benchmarks>

Que voit un attaquant de votre organisation ?

Avant de durcir, voyez ce qui est visible de l'extérieur. Sedona Radar vérifie la partie exposée sur Internet : enregistrements SPF, DKIM et DMARC, services accessibles. Il ne voit pas la configuration interne de votre locataire. Lancez un scan gratuit, sans engagement.

[Lancer mon scan gratuit](#)

sedona-ai.com/scan-gratuit