Hardening Microsoft Entra ID 2026 : Guide Complet de Sécurisation

> Guide complet de sécurisation Microsoft Entra ID 2026 — Conditional Access, PIM, FIDO2, CAE, protection OAuth, Identity Protection et checklist 20 points.

Microsoft Entra ID (anciennement Azure Active Directory) est le système de gestion des identités cloud au cœur de l'écosystème Microsoft 365. En 2026, la quasi-totalité des organisations françaises utilisant Microsoft 365 ont leur authentification et leur gestion d'accès centralisées dans Entra ID — ce qui en fait la cible la plus stratégique pour les attaquants cherchant à compromettre un SI Microsoft. Les techniques d'attaque Entra ID spécifiques (illicit consent grants, token theft, device code phishing, AiTM attaques bypassing MFA classique, abus des applications OAuth) ont considérablement évolué depuis 2022 et requirent des mesures de sécurisation avancées bien au-delà de la simple activation du MFA. Ce guide complet présente les mesures de durcissement (**hardening**) Microsoft Entra ID indispensables en 2026 : Conditional Access avancé, Privileged Identity Management (PIM), méthodes d'authentification FIDO2 et passwordless, protection de l'identité (Identity Protection), Continuous Access Evaluation (CAE), configuration des politiques de session, sécurisation des applications OAuth, et protection contre les vecteurs d'attaque spécifiques à Entra ID. Chaque section inclut des configurations concrètes applicables dans le portail Entra ou via Microsoft Graph PowerShell.

À RETENIR

Points clés à retenir

L'activation du MFA seul est insuffisante en 2026 : les attaques AiTM (Evilginx, Modlishka) contournent le MFA TOTP classique

FIDO2/Passkeys et Certificate-Based Authentication sont les seules méthodes résistantes au phishing à déployer pour les comptes sensibles

Privileged Identity Management (PIM) doit être activé pour tous les rôles d'administrateur Entra — just-in-time access uniquement

Le Conditional Access avec Sign-in Risk + User Risk (Identity Protection) est le contrôle compensatoire le plus efficace

Les **Continuous Access Evaluation (CAE)** révoquent les tokens en temps réel — activer pour toutes les applications compatibles

L'audit des applications OAuth est critique : de nombreuses organisations ont des apps OAuth malveillantes avec accès à leurs données Microsoft 365

Pourquoi le MFA Classique Ne Suffit Plus en 2026

La compromission de comptes Microsoft 365 via des attaques contournant le MFA TOTP (Time-based One-Time Password) est devenue l'un des vecteurs d'attaque les plus fréquents en 2026. Les frameworks AiTM (Adversary-in-the-Middle) comme Evilginx2, Modlishka, et Muraena déploient des proxies transparents qui interceptent à la fois les credentials et les cookies de session MFA — permettant à l'attaquant de réutiliser le cookie de session volé sans avoir à refaire le challenge MFA.

> ⚡ **Retour terrain**
>
> Dans les projets IAM, le cas le plus fréquent que je rencontre est celui des comptes de service sans propriétaire identifié — créés pour un projet terminé ou un prestataire parti, et jamais supprimés. Pour une banque régionale, l'inventaire a identifié 134 comptes de service sans propriétaire actif, dont 23 avaient des droits administrateurs locaux sur des serveurs de production. La désactivation progressive de ces comptes sur 6 semaines n'a déclenché aucune anomalie applicative.

Le fonctionnement d'une attaque AiTM contre Microsoft 365 : l'utilisateur est dirigé (via un email de phishing) vers un site AiTM qui ressemble au portail Microsoft 365. Quand l'utilisateur entre ses credentials et complète le MFA (via TOTP ou notification push), le proxy AiTM relaie ces informations au vrai Microsoft 365 et récupère le cookie de session Microsoft authentifié. L'attaquant peut ensuite utiliser ce cookie de session (valide 24h par défaut) pour accéder au compte Microsoft 365 de la victime sans MFA — le cookie est déjà authentifié. Ce vecteur d'attaque rend le MFA TOTP (Google Authenticator, Microsoft Authenticator en mode notification push) insuffisant pour les comptes sensibles.

Les seules méthodes d'authentification résistantes au phishing et aux attaques AiTM sont : **FIDO2 / Passkeys** (WebAuthn bound to the origin — le token FIDO2 vérifie que le domaine auquel il s'authentifie correspond exactement au domaine légitime, rendant les proxies AiTM

inefficaces), **Certificate-Based Authentication (CBA)** (certificat client stocké dans la carte à puce ou un TPM), et **Windows Hello for Business** (credential basé sur une paire de clés asymétriques liée au device et au TPM). Ces méthodes doivent être déployées prioritairement pour les administrateurs Entra et les utilisateurs à haut risque.

Conditional Access : Architecture des Politiques de Sécurité Entra

Le Conditional Access (Accès Conditionnel) est le moteur de politique de sécurité central d'Entra ID. Il évalue les conditions de chaque tentative d'accès (identité, device, localisation, risque) et applique des contrôles (MFA, blocage, session limitée, device compliance). La conception d'une architecture Conditional Access efficace est l'une des tâches les plus importantes du durcissement Entra ID.

Les politiques Conditional Access fondamentales à implémenter : **MFA pour tous les utilisateurs** (sauf exceptions justifiées) ; **Require Compliant Device ou Hybrid Azure AD Joined** pour l'accès aux applications sensibles (seuls les devices managés et conformes peuvent accéder) ; **Block Legacy Authentication** (bloquer tous les protocoles legacy — SMTP AUTH, POP3, IMAP4, MAPI over HTTP — qui ne supportent pas le MFA) ; **Require MFA for Azure Management** (MFA obligatoire pour l'accès à Azure Portal et aux APIs de management) ; et **Session Controls** (Sign-in frequency limitée pour les accès sans device compliant, Sign-out after inactivity).

Les politiques avancées (Microsoft Entra ID P2 requis) : **Sign-in Risk Policy** (bloquer ou forcer la réauthentification si le risque de connexion est Medium ou High — basé sur les signaux Identity Protection) ; **User Risk Policy** (forcer la réinitialisation de mot de passe si le risque utilisateur est élevé — email de l'utilisateur détecté dans des leaks de credentials) ; et **Authentication Strengths** (requérir des méthodes MFA résistantes au phishing — FIDO2, CBA, WHfB — pour les accès aux applications les plus sensibles).

PIM : Gestion des Accès Privilégiés Entra ID

Privileged Identity Management (PIM) est la fonctionnalité Entra ID P2 qui implémente le principe de moindre privilège temporel pour les rôles d'administrateur Entra ID et Azure. Au lieu d'attribuer des rôles d'administrateur permanent (standing access), PIM attribue des **eligible assignments** — l'administrateur doit activer explicitement son rôle pour une durée limitée (1 à 8h typiquement) lorsqu'il en a besoin.

Les avantages de PIM pour la sécurité Entra ID : réduction de la fenêtre d'exploitation en cas de compromission d'un compte administrateur (le rôle n'est pas actif en permanence), audit complet des activations de rôles (qui a activé quel rôle, quand, pour quelle justification), et approbation requise pour les activations de rôles critiques (Global Administrator, Privileged Role Administrator). La configuration PIM recommandée : imposer une justification écrite pour toute activation, activer les notifications email au propriétaire du rôle lors de chaque activation, configurer des alertes PIM pour les activations hors des heures de bureau, et réviser les eligible assignments trimestriellement.

Les rôles à traiter en priorité dans PIM : **Global Administrator** (rôle le plus puissant, à avoir maximum 2-3 comptes eligible, jamais en standing access), **Privileged Role Administrator** (gestion des rôles, aussi critique que Global Admin), **User Administrator**, **Application Administrator**, **Exchange Administrator**, et **SharePoint Administrator**. Tous les rôles avec portée de données (accès aux données utilisateurs ou aux configurations de sécurité) doivent être migrés de permanent à eligible via PIM.

Entra Identity Protection : Détection des Risques en Temps Réel

Microsoft Entra Identity Protection analyse en temps réel les connexions à Entra ID pour détecter des comportements suspects et calculer des scores de risque (Sign-in Risk et User Risk). Ces scores sont basés sur des centaines de signaux : IP addresses sur des listes noires Microsoft, connexions depuis des anonymizing proxies (TOR, VPN), voyage impossible (connexions

depuis deux pays impossibles à la même heure), passwords détectés dans des leaks (User Risk), et utilisation de malware connu.

La configuration d'Identity Protection recommandée : activer les politiques automatisées de réponse aux risques via Conditional Access (Sign-in Risk High → bloquer, Sign-in Risk Medium → MFA renforcé, User Risk High → forcer la réinitialisation de mot de passe) ; configurer les alertes vers le SOC pour les détections de risques (via Logic Apps ou Sentinel) ; et effectuer des revues hebdomadaires des utilisateurs détectés à risque pour investiguer manuellement les faux positifs potentiels. Les rapports Identity Protection (Risky Sign-ins, Risky Users) sont exportables vers Sentinel pour la corrélation avec d'autres signaux de sécurité.

Continuous Access Evaluation (CAE) : Révocation des Tokens en Temps Réel

Continuous Access Evaluation (CAE) est un mécanisme Microsoft qui permet à Entra ID de révoquer des tokens d'accès en temps réel — sans attendre l'expiration naturelle du token (qui peut durer jusqu'à 24h par défaut). CAE est activé par défaut pour les applications Microsoft 365 (Exchange Online, SharePoint, Teams) et peut être étendu aux applications tiers qui supportent le protocole.

Quand CAE révoque-t-il un token ? Lorsqu'un compte utilisateur est désactivé ou supprimé dans Entra ID (révocation quasi-immédiate), lorsqu'un mot de passe est réinitialisé, lorsque le risque utilisateur ou connexion monte à High (Identity Protection), ou lorsqu'une politique Conditional Access est modifiée de façon à bloquer la session existante. En pratique, CAE signifie que si un compte compromis est désactivé, l'attaquant qui disposait d'un token de session valide ne pourra plus accéder aux données Microsoft 365 en quelques minutes — plutôt qu'en 24h avec les tokens classiques.

La configuration CAE dans les politiques Conditional Access : dans les politiques Conditional Access, sous "Session", activer "Customize continuous access evaluation" en mode "Strict" pour imposer une réévaluation immédiate des tokens à chaque accès, plutôt qu'uniquement sur signaux critiques. Cette configuration augmente légèrement la charge sur les serveurs

d'authentification Microsoft mais maximise la sécurité et réduit significativement la fenêtre d'exploitation pour les tokens volés — un compromis très favorable pour les applications contenant des données sensibles comme Exchange Online ou SharePoint.

Sécurisation des Applications OAuth et Consentements

Les attaques par "illicit consent grant" (consentement OAuth frauduleux) sont devenues l'un des vecteurs d'attaque les plus insidieux contre Microsoft 365 en 2026. Le principe : l'attaquant enregistre une application OAuth sur un tenant Azure, puis envoie à des utilisateurs ciblés un email de phishing les incitant à "autoriser" cette application sur leur compte Microsoft 365. Si l'utilisateur clique et consent, l'application malveillante obtient un accès permanent et délégué aux données de l'utilisateur (emails, fichiers OneDrive, contacts) sans MFA requis — car le consentement OAuth contourne le Conditional Access traditionnel.

Les contre-mesures contre les attaques de consentement OAuth : **désactiver le consentement utilisateur** (Entra Admin Center → Enterprise Applications → Consent and Permissions → "Do not allow user consent") pour forcer tous les consentements d'applications à passer par des administrateurs ; **activer le workflow de consentement administrateur** pour permettre aux utilisateurs de demander l'approbation d'une application tout en attendant la validation administrative ; **auditer régulièrement les applications autorisées** (Entra Admin Center → Enterprise Applications → All Applications → filtre "User consent") pour détecter des applications inconnues avec des permissions excessives ; et **restreindre les applications autorisées à un catalogue approuvé** via les politiques Conditional Access (filter for applications).

La commande Microsoft Graph PowerShell pour auditer les consentements OAuth existants :

```
# Lister tous les OAuth2PermissionGrants (consentements utilisateur)

Connect-MgGraph -Scopes "Directory.Read.All"

Get-MgOauth2PermissionGrant -All | Select-Object ClientId, ConsentType, Scope,
PrincipalId | Export-Csv oauth_consents.csv

# Identifier les apps avec scope Mail.Read ou Files.ReadWrite
```

```
Get-MgOauth2PermissionGrant -All | Where-Object {$_.Scope -match "Mail|Files"}
| Select ClientId, Scope
```

Device Code Phishing : Le Nouveau Vecteur AiTM

Le "Device Code Phishing" (également appelé "Device Authorization Grant abuse") est une technique d'attaque qui exploite le flux d'authentification OAuth "device code" — conçu pour les appareils sans navigateur (TV, imprimantes) — pour voler des tokens Entra ID sans credential de l'utilisateur. L'attaquant génère un device code via l'API Microsoft, puis envoie à sa victime un email demandant d'entrer ce code sur `microsoft.com/devicelogin` pour "vérifier son identité". Si la victime entre le code, l'attaquant récupère un token Entra ID valide et authentifié avec les droits de la victime, sans jamais voir son mot de passe.

La contre-mesure principale : bloquer le flux Device Code via Conditional Access. Dans une politique Conditional Access, sous "Conditions → Authentication flows", sélectionner "Device code flow" et bloquer pour tous les utilisateurs (ou à minima pour les utilisateurs non-exclus explicitement comme des comptes de service sur TV/IoT). Pour les organisations avec des applications légitimes utilisant le Device Code flow (Teams Rooms, écrans de salle de réunion), créer des exceptions ciblées. Notre article sur la mise en place du MFA résistant au phishing détaille les configurations Conditional Access pour contrer l'ensemble des vecteurs d'attaque AiTM et Device Code.

Politique de Mots de Passe et Authentification Passwordless

La politique de mots de passe Entra ID a évolué significativement depuis les recommandations historiques du NIST (SP 800-63B) : l'exigence de complexité (majuscule + chiffre + symbole) combinée à une rotation forcée courte (90 jours) est désormais reconnue comme contre-productive — elle pousse les utilisateurs à des mots de passe faibles et prévisibles (P@ssw0rd!, Mois+Année). Les recommandations actuelles (ANSSI, NIST, Microsoft) favorisent des mots de

passe longs et uniques (16+ caractères) sans rotation forcée sauf en cas de compromission connue, combinés avec du MFA.

L'objectif ultime en matière d'authentification est le **passwordless** — éliminer complètement les mots de passe pour les utilisateurs. Microsoft propose trois voies de déploiement passwordless : **Windows Hello for Business** (biométrie ou PIN lié au device, pour les utilisateurs Windows managés), **Microsoft Authenticator App passwordless** (notification push avec biométrie sur smartphone), et **FIDO2 Security Keys** (clé physique USB/NFC, la plus résistante au phishing). Le déploiement passwordless complet est un projet de 6 à 18 mois selon la taille de l'organisation, mais il peut commencer par les comptes les plus sensibles (administrateurs, utilisateurs accédant à des données critiques) avant d'être étendu progressivement.

Sécurisation des Comptes d'Urgence (Break Glass Accounts)

Les comptes d'urgence (emergency access accounts, ou "break glass" accounts) sont des comptes Global Administrator Entra ID configurés pour être accessibles même si toutes les autres méthodes d'accès sont compromises ou indisponibles (panne de l'IdP, boucle dans les politiques Conditional Access, perte d'accès à tous les comptes administrateurs). Ces comptes sont indispensables pour la résilience opérationnelle mais constituent également un risque de sécurité s'ils sont mal configurés.

La configuration recommandée des comptes d'urgence : créer **deux comptes** (pour la redondance), utiliser des adresses email non liées à des personnes physiques (ex : `urgence1@domaine.fr`), stocker les credentials dans un coffre physique sécurisé (pas uniquement dans un coffre-fort numérique qui pourrait être inaccessible lors d'une panne Entra), **exclure ces comptes** de toutes les politiques Conditional Access (sinon le mécanisme de break glass est compromis), mais **monitorer toute utilisation** de ces comptes via des alertes immédiates (Azure Monitor + Logic App → email/Teams au RSSI dès qu'un compte break glass est utilisé). Ces comptes ne doivent être utilisés qu'en cas d'urgence réelle et leur utilisation doit être systématiquement documentée.

Audit et Reporting Entra ID : Microsoft Sentinel Integration

L'audit des activités Entra ID est la source de vérité pour la détection des incidents de sécurité identité. Les logs Entra ID doivent être exportés vers un SIEM pour la conservation à long terme (Entra ID conserve les Sign-in logs 30 jours en P1 et 90 jours en P2 — insuffisant pour l'investigation forensique) et pour la corrélation avec d'autres sources de logs.

La configuration de l'export des logs Entra vers Microsoft Sentinel : dans le portail Azure, Entra ID → Monitoring → Diagnostic settings → Create diagnostic setting, sélectionner tous les logs (AuditLogs, SignInLogs, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, RiskyUsers, UserRiskEvents) et rediriger vers votre workspace Log Analytics Sentinel. Une fois dans Sentinel, les Analytique Rules sur les logs Entra permettent de détecter les attaques MITRE ATT&CK Identity (T1078, T1136, T1098) avec des délais d'alerte de quelques minutes. Notre article sur l'implémentation de Microsoft Sentinel comme SIEM couvre la configuration complète des sources de données et des analytiques pour la détection des incidents Entra ID.

Risque	Contre-mesure principale	Licence requise
AiTM / Phishing MFA	FIDO2 / CBA (phishing-resistant MFA) pour comptes sensibles	Entra P1
Compromission compte admin	PIM — accès just-in-time pour tous les rôles admin	Entra P2
Token theft / session hijack	CAE (Continuous Access Evaluation) + Token Protection	Entra P1
Credentials spray / brute force	Smart Lockout + Identity Protection + Sign-in Risk CA	Entra P2
Illicit consent grant	Bloquer user consent, workflow approbation admin	Entra P1
Device Code Phishing	CA → bloquer Device Code flow pour les utilisateurs	Entra P1
Legacy auth protocols	CA → bloquer toute authentification legacy (SMTP AUTH, IMAP)	Entra Free
Guest access non contrôlé	External Identities settings + Access Reviews + CA Guest policies	Entra P2

Gestion des Identités Externes (Guest) et B2B

Les identités guest (utilisateurs externes invités dans votre tenant Entra ID via la collaboration B2B) représentent une surface d'attaque souvent négligée. Ces comptes ont accès à vos données Microsoft 365 (Teams, SharePoint, OneDrive) mais sont contrôlés par des tenants externes dont vous ne maîtrisez pas les politiques de sécurité — un compte guest peut appartenir à un tenant externe sans MFA activé, sans Conditional Access, et avec une posture de sécurité médiocre.

Les mesures de durcissement pour les identités B2B guest : configurer une **politique Conditional Access spécifique aux guests** qui impose le MFA (en complément du MFA du tenant d'origine) pour l'accès à vos ressources ; limiter les permissions des guests aux ressources strictement nécessaires (pas d'accès à l'annuaire Entra, pas de création de groupes, pas d'invitation d'autres guests) ; configurer des **Access Reviews** trimestrielles automatiques pour réviser et supprimer les guests inactifs ou inutiles (les comptes B2B dormants sont une source d'exposition) ; et limiter les domaines autorisés pour les invitations B2B (allowlist de domaines partenaires approuvés) via les "External collaboration settings" dans Entra ID.

Sécurité des Workload Identities : Service Principals et Managed Identities

Au-delà des identités humaines, Entra ID gère également les identités des applications et des services cloud — les **Service Principals** (identités d'applications enregistrées dans Entra) et les **Managed Identities** (identités attribuées automatiquement aux ressources Azure par Microsoft). Ces "workload identities" ont souvent des permissions élevées et sont moins surveillées que les comptes utilisateurs humains.

Les risques des workload identities non sécurisées : des Service Principals avec des permissions excessives (Global Reader, User.ReadWrite.All) créés pour des intégrations qui n'ont plus besoin de ces permissions, des secrets d'application (client secrets) qui n'expirent jamais (ou qui ont été générés il y a des années sans rotation), et des applications enregistrées par des développeurs avec des permissions très larges pour faciliter le développement (et jamais restrictées pour la

production). Le durcissement des workload identities passe par : audit régulier des permissions de tous les Service Principals (via Microsoft Graph Explorer ou PowerShell), rotation régulière des secrets d'application (ou migration vers des Managed Identities qui éliminent la gestion des secrets), et Application access policies pour limiter les permissions des applications multi-tenant.

Microsoft Secure Score Entra : Prioriser les Actions à Fort Impact

Le Microsoft Secure Score (accessible depuis le portail Microsoft Defender XDR ou depuis Entra Admin Center) est un tableau de bord qui évalue la posture de sécurité de votre tenant Microsoft 365 sur une échelle de 0 à 100% et fournit une liste priorisée d'actions d'amélioration avec leur impact estimé sur le score. C'est un outil précieux pour structurer et prioriser un programme de hardening Entra ID.

Les actions du Secure Score à plus fort impact pour Entra ID en 2026 : **"Enable MFA for all users" (+10-20 points)** — activer le MFA pour 100% des comptes si pas encore fait ; **"Do not allow users to consent to apps accessing company data" (+5-10 points)** — bloquer le consentement utilisateur pour les applications OAuth ; **"Enable Identity Protection sign-in risk policy" (+5-10 points)** — configurer la politique CA basée sur le risque de connexion ; **"Ensure all administrators have MFA enabled" (+5 points)** — vérifier que tous les comptes avec des rôles admin ont le MFA activé ; et **"Use privileged identity management to enable just-in-time privileged access" (+5 points)** — activer PIM pour les rôles admin. Le Secure Score se met à jour quotidiennement et permet de suivre la progression du programme de hardening dans le temps — une métrique de reporting utile pour le RSSI et le COMEX.

Un point important sur le Secure Score : le score est relatif aux recommandations Microsoft actuelles et ne reflète pas nécessairement tous les risques de votre environnement spécifique. Un tenant avec un score de 90% peut encore avoir des risques non couverts par le Secure Score (mauvaise gestion des workload identities, lacunes dans les logs, politiques CA mal calibrées). Le Secure Score est un point de départ, pas un objectif final absolu — l'objectif est de traiter les risques réels de votre environnement, pas d'optimiser le score.

Gestion des Shared Mailboxes et Comptes de Service M365

Les boîtes aux lettres partagées (Shared Mailboxes) et les comptes de service Microsoft 365 (comptes sans utilisateur humain associé, utilisés par des applications ou des automatisations) représentent une catégorie de comptes souvent mal sécurisée dans les tenants Entra ID. Ces comptes ont souvent le MFA désactivé (pour permettre aux applications d'y accéder), des mots de passe faibles ou non rotés depuis des années, et pas de surveillance des connexions.

Les bonnes pratiques pour sécuriser les comptes de service et shared mailboxes dans Entra ID : utiliser des **Managed Identities** pour les applications Azure qui s'authentifient à Microsoft 365 (élimine le besoin d'un compte de service avec mot de passe) ; pour les shared mailboxes, **bloquer la connexion interactive** (via "Sign-in blocked" dans les propriétés du compte) et n'autoriser l'accès qu'en mode délégué depuis des comptes utilisateurs authentifiés avec MFA ; configurer des **alertes de connexion** sur les comptes de service (toute connexion interactive sur un compte de service devrait déclencher une alerte SOC car elle est anormale) ; et effectuer un inventaire annuel des comptes de service actifs pour révoquer les comptes dont l'application associée n'existe plus ou n'en a plus besoin. Le respect de ces bonnes pratiques réduit significativement le risque d'attaque par credential stuffing ou brute force sur ces comptes exposés.

Checklist Hardening Entra ID : 20 Points de Contrôle

Voici les 20 points de contrôle indispensables pour évaluer et améliorer la posture de sécurité Entra ID. Cette checklist peut servir de base pour un audit de sécurité Entra ID ou un plan de remédiation.

Authentification (5 points) : MFA activé pour 100% des utilisateurs (pas uniquement via Security Defaults) ; Legacy authentication bloqué via Conditional Access ; FIDO2/CBA déployé pour tous les administrateurs ; Passwordless activé pour au moins 20% des utilisateurs ; politique de password configurée (pas de rotation forcée courte, bannissement des mots de passe compromis via Password Protection).

Accès Privilégiés (4 points) : PIM activé pour tous les rôles d'admin Entra et Azure ; aucun compte Global Admin permanent (tous en eligible via PIM) ; comptes break glass configurés avec monitoring ; Access Reviews configurées pour les rôles sensibles (trimestriel minimum).

Conditional Access (4 points) : politiques CA couvrant 100% des utilisateurs ; Sign-in Risk et User Risk policy configurées (P2) ; Device Compliance requise pour les apps sensibles ; Device Code flow bloqué.

Applications et OAuth (4 points) : consentement utilisateur désactivé (admin approval uniquement) ; audit des OAuth grants existants réalisé ; User consent workflow configuré ; applications tierces auditées et non utilisées révoquées.

Monitoring (3 points) : logs Entra exportés vers Sentinel ou SIEM ; alertes configurées pour les événements critiques (activation rôle Global Admin, ajout Global Admin, guest invitation massive) ; rapport Identity Protection reviewed hebdomadairement.

La réalisation de cette checklist peut se faire via une combinaison du Microsoft Secure Score (pour les 15 premiers points — la plupart ont un équivalent dans le Secure Score), d'un script PowerShell d'audit automatisé (pour les vérifications non couvertes par le Secure Score), et d'une revue manuelle trimestrielle par le RSSI ou un prestataire de sécurité spécialisé Microsoft 365. Le résultat de chaque revue checklist doit être documenté avec la date, le responsable, et les non-conformités détectées avec leur plan de remédiation — cette documentation prouve la diligence en cas d'audit NIS2 ou de sinistre cyber. Les 5 points de monitoring sont particulièrement importants : une organisation qui a une posture Entra bien configurée mais sans monitoring des alertes n'a pas de capacité de détection des incidents identité — elle découvrira la compromission uniquement lorsque l'attaquant déploiera son ransomware, soit des semaines ou des mois après l'intrusion initiale.

Token Protection et Binding des Tokens à l'Appareil

Le vol de tokens d'accès (Token Theft) est une technique d'attaque croissante en 2026 : un attaquant qui parvient à extraire un token d'accès Entra ID valide depuis un endpoint (via malware, memory dump, ou exfiltration d'un cookie de navigateur) peut l'utiliser depuis

n'importe où sans avoir besoin du mot de passe ou du MFA de la victime. Le token est comme un pass d'entrée qui peut être copié et réutilisé.

Token Protection (en preview dans Entra ID depuis 2023, disponibilité GA progressive en 2025-2026) est la réponse Microsoft à cette menace : il lie cryptographiquement le token d'accès à l'appareil qui l'a obtenu, via une clé privée stockée dans le TPM de l'appareil. Un token "protégé" ne peut être utilisé que depuis l'appareil qui l'a généré — le voler et l'utiliser depuis un autre appareil est impossible car la preuve de possession de la clé TPM ne peut pas être présentée. La configuration Token Protection se fait dans les politiques Conditional Access, sous "Session → Require token protection for sign-in sessions". Elle nécessite des clients Windows 11 récents avec TPM 2.0 et les applications Office 365 récentes (Office 365 build 16.0+). Le déploiement est progressif — commencer par les accès Exchange Online et SharePoint pour les utilisateurs les plus sensibles.

Cross-Tenant Access Settings : Sécuriser les Collaborations B2B

Les "Cross-Tenant Access Settings" (paramètres d'accès inter-tenants) d'Entra ID permettent de contrôler finement les collaborations B2B avec d'autres organisations Microsoft 365 — à la fois les accès entrants (utilisateurs d'autres organisations qui accèdent à vos ressources) et les accès sortants (vos utilisateurs qui accèdent aux ressources d'autres organisations).

Les configurations Cross-Tenant Access critiques pour le hardening Entra : **Inbound settings** (accès entrant) — par défaut, Entra ID accepte les invitations d'utilisateurs de n'importe quel autre tenant Microsoft ; en durcissement, restreindre les tenants autorisés à la liste des partenaires approuvés (allowlist de tenant IDs) ; **Outbound settings** (accès sortant) — contrôler quelles applications de votre tenant vos utilisateurs peuvent partager avec l'extérieur (éviter que des fichiers SharePoint confidentiels soient partagés avec n'importe quel utilisateur Microsoft) ; et **B2B Direct Connect** (accès direct sans invitation, pour les partenaires proches) — à configurer uniquement pour des organisations spécifiques approuvées. La revue et la configuration des Cross-Tenant Access Settings est une étape souvent oubliée dans les projets de hardening Entra, alors qu'elle est essentielle pour les organisations avec de nombreux partenaires et prestataires.

Named Locations et Politiques de Géolocalisation

Les "Named Locations" dans Conditional Access permettent de définir des zones géographiques ou des plages d'adresses IP de confiance, et d'utiliser ces définitions dans les politiques d'accès. La géolocalisation est un signal important pour la détection des connexions anormales et pour les politiques de blocage des accès depuis des pays non utilisés par l'organisation.

La configuration recommandée des Named Locations : créer des locations IP pour les plages d'adresses de votre réseau corporate (bureaux, VPN corporate) et les marquer comme "trusted locations" (réduire les exigences MFA pour les connexions depuis ces IPs si souhaité) ; et créer une politique CA "Block access from countries outside France/EU" pour les organisations dont les utilisateurs ne voyagent jamais hors EU (bloque les connexions depuis des pays comme la Russie, la Chine, la DPRK, sources statistiquement fréquentes d'attaques ciblées). Cette politique doit avoir des exceptions pour les utilisateurs légitimement en déplacement international (via un groupe d'utilisateurs "International Travelers" qui bypasse la restriction géographique avec un MFA renforcé).

Entra ID Verified ID : Credentials Décentralisées et Vérifiables

Microsoft Entra Verified ID est une fonctionnalité basée sur les standards W3C Verifiable Credentials et Decentralized Identifiers (DIDs) qui permet d'émettre et de vérifier des credentials numériques vérifiables. Bien que moins directement lié au hardening opérationnel, Verified ID ouvre des cas d'usage de sécurité avancés qui vont devenir plus courants en 2026-2027.

Les cas d'usage Verified ID pertinents pour la sécurité d'entreprise : **Face Check pour la réactivation de comptes** — quand un utilisateur perd l'accès à ses credentials MFA, au lieu d'un processus de réactivation manuel (appel au helpdesk, vérification d'identité approximative), Verified ID avec face check peut vérifier biométriquement l'identité de l'utilisateur contre un document d'identité vérifié avant de réinitialiser les credentials ; **accès partenaires vérifiés** — plutôt que d'inviter des partenaires B2B avec des credentials non-vérifiés, exiger que les partenaires présentent un Verified ID (credential émis par leur organisation ou par un vérificateur

d'identité) pour accéder à des ressources sensibles ; et **vérification des attributs sans partage de données** — prouver qu'un utilisateur appartient à un groupe ou a un rôle spécifique sans révéler toutes ses données d'identité (privacy-preserving access control).

Intégration Entra ID avec les SOC et SOAR

L'intégration d'Entra ID dans l'écosystème SOC est indispensable pour une réponse aux incidents identité efficace. Les incidents identité Entra (compte compromis, escalade de privilèges, OAuth malveillant) doivent être détectés et traités avec la même vitesse et la même rigueur que les incidents réseau ou endpoint.

L'intégration SOC Entra ID recommandée : **connecteur Microsoft Entra vers Microsoft Sentinel** (natif, configuration en quelques clics) pour ingérer tous les logs d'audit et de connexion Entra dans Sentinel ; **playbooks SOAR** pour les réponses automatisées aux incidents Entra courants — par exemple, un playbook qui désactive automatiquement un compte si l'Identity Protection détecte un risque utilisateur "High" et qu'aucun analyste ne l'a traité dans les 2h ; **hunting queries Sentinel** pour la recherche proactive des indicateurs de compromission Entra (nouveaux Global Admins, modifications de politiques CA, nouveaux OAuth grants sur des comptes sensibles). Notre article sur l'implémentation Zero Trust Microsoft 365 couvre l'architecture complète de la défense Microsoft 365, incluant l'intégration Entra ID - Sentinel - Defender XDR pour une protection en profondeur.

Entra ID et Conformité NIS2 : Cartographie des Exigences

La directive NIS2 impose des mesures de sécurité de gestion des accès et d'authentification dans l'article 21. Le durcissement Entra ID contribue directement à satisfaire plusieurs de ces exigences pour les entités soumises à NIS2.

La cartographie des mesures Entra ID → exigences NIS2 : **MFA obligatoire** (NIS2 art. 21 - authentification forte) → MFA Entra + FIDO2 pour les accès aux systèmes critiques ; **gestion des accès privilégiés** (NIS2 art. 21 - contrôle d'accès) → PIM pour les rôles Entra/Azure, revue des droits trimestrielle ; **politiques de contrôle d'accès** (NIS2 art. 21 - politiques de sécurité) → Conditional Access policies documentées et testées ; **journalisation et monitoring** (NIS2 art. 21 - surveillance) → logs Entra vers Sentinel, conservation >12 mois. Les entités soumises à NIS2 doivent pouvoir démontrer ces mesures lors d'un contrôle de l'ANSSI — documenter les configurations Entra dans un dossier de sécurité est une bonne pratique de conformité.

Entra ID External Authentication Methods : Intégration MFA Tiers

Certaines organisations ont investi dans des solutions MFA tiers (Duo Security, RSA SecurID, Ping Identity) avant la maturité des fonctionnalités MFA natives Entra ID. La fonctionnalité "External Authentication Methods" (EAM) d'Entra ID (disponible depuis 2024) permet d'intégrer ces solutions MFA tiers directement dans le flux d'authentification Entra, sans passer par les legacy "custom controls" qui avaient des limitations importantes.

EAM permet à Entra ID de déléguer la vérification MFA à un système externe (Duo, Ping) via un protocole standardisé, tout en maintenant les politiques Conditional Access Entra (les policies CA peuvent référencer les méthodes EAM comme satisfaisant les exigences MFA). Cela permet aux organisations de migrer progressivement vers les méthodes MFA natives Entra (Microsoft Authenticator, FIDO2) sans forcer une migration instantanée depuis leur solution MFA tiers existante. La configuration EAM se fait dans Entra Admin Center → Security → Authentication Methods → External Authentication Methods.

Anecdote Terrain : Le Consentement OAuth Fantôme

En 2025, lors d'un audit Entra ID pour une ETI du secteur retail de 400 employés, nous avons découvert via l'audit des OAuth grants une application inconnue ayant obtenu le consentement de

87 utilisateurs avec les scopes `Mail.Read`, `Files.ReadWrite.All`, et `Contacts.Read`. L'application avait été enregistrée 8 mois auparavant et avait accédé en continu aux emails et fichiers de ces 87 utilisateurs — dont 3 membres de la direction et le directeur financier.

L'enquête a révélé que les utilisateurs avaient été victimes d'une campagne de phishing par illicit consent grant, aucun n'avait remarqué avoir accordé ces permissions (l'UI Microsoft pour le consentement OAuth est suffisamment trompeuse pour qu'un utilisateur lambda ne réalise pas l'importance de ce qu'il consent). La rétraction des permissions (révoquer tous les OAuth grants de l'application malveillante) a été faite en quelques minutes via PowerShell, mais les données (8 mois d'emails de la direction) avaient déjà été exfiltrées. La prévention par configuration (bloquer le user consent) aurait évité l'incident à zéro coût.

FAQ — Questions sur le Hardening Entra ID

Quelle licence Entra ID est nécessaire pour un bon niveau de sécurité ?

Entra ID P2 (inclus dans Microsoft 365 E5 ou Microsoft Entra ID P2 standalone) est nécessaire pour les fonctionnalités de sécurité les plus importantes : PIM (Privileged Identity Management), Identity Protection (Sign-in Risk + User Risk), Access Reviews, et Entitlement Management. Entra ID P1 (M365 E3, Business Premium) couvre Conditional Access et MFA mais sans les fonctionnalités risk-based. Pour les PME avec un budget limité, Microsoft 365 Business Premium (qui inclut Entra P1 + Defender for Business) est souvent le meilleur équilibre coût/sécurité.

Comment migrer vers le MFA résistant au phishing sans perturber les utilisateurs ?

La migration vers FIDO2 ou Windows Hello for Business doit être progressive. Commencer par les comptes les plus sensibles (administrateurs Entra, direction, équipes finance/RH avec accès aux données critiques) qui justifient l'investissement en formation et matériel (clé FIDO2 Yubikey, ~50 euros). Déployer Windows Hello for Business en parallèle sur les postes Windows 10/11 managés — c'est transparent pour l'utilisateur (biométrie + PIN) et ne requiert pas d'achat

de matériel supplémentaire. Utiliser les "Authentication Strengths" dans Conditional Access pour imposer FIDO2/WHfB uniquement pour les accès aux applications les plus sensibles dans un premier temps.

Entra ID Security Score : à quel score viser ?

Le Secure Score Microsoft Entra (accessible dans le portail Entra Admin Center → Security → Secure Score) évalue la posture de sécurité de votre tenant sur ~100 points. Un score supérieur à 70% est considéré comme bon. Les actions à plus fort impact sur le score : activer PIM pour les rôles admin (+5-15 points), activer le MFA pour tous les admins (+10-20 points), bloquer l'authentification legacy (+5-10 points), activer Identity Protection (+5-10 points). Revenir régulièrement sur le Secure Score est une bonne pratique pour identifier les nouvelles recommandations ajoutées par Microsoft.

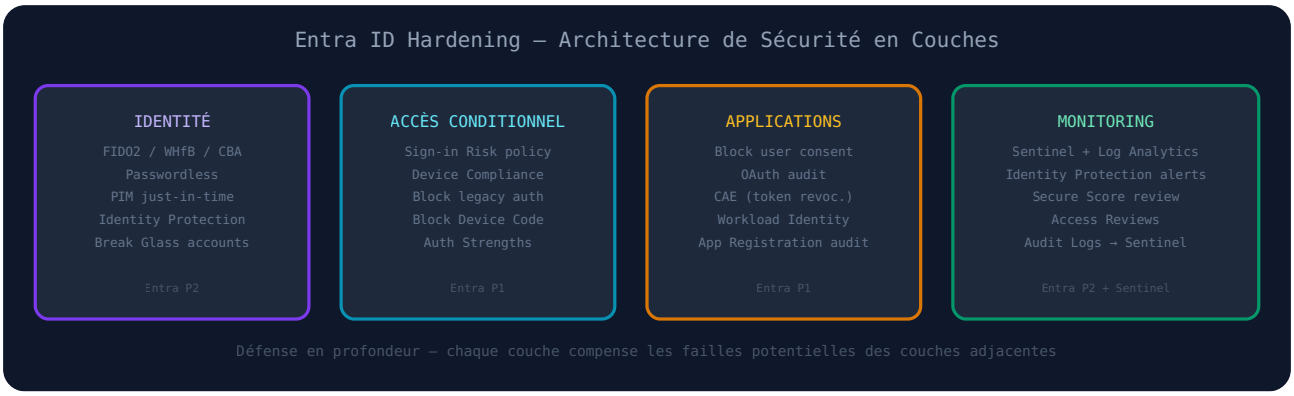
Comment détecter si notre tenant Entra a été compromis ?

Les indicateurs de compromission Entra ID à surveiller : connexions depuis des pays inhabituels (surtout pour les comptes admin), ajout de nouveaux Global Admins ou modifications de rôles sensibles hors procédure normale, création de nouveaux Service Principals avec des permissions larges, nouveaux OAuth grants sur des comptes sensibles (surtout Mail.Read, EWS.AccessAsUser), modifications des politiques Conditional Access (contournement de contrôles), et alertes Identity Protection (Risky Sign-ins, Risky Users). Le rapport "Unified Audit Log" de Microsoft Purview est la source de logs complète pour détecter ces événements. Notre article sur la sécurité et l'audit Microsoft 365 couvre les techniques d'audit et de monitoring des tenants Microsoft 365.

Comment sécuriser les comptes admin Entra ID qui utilisent encore des credentials email/password ?

Migration prioritaire vers des comptes admin dédiés (pas les comptes utilisateurs habituels avec une boîte mail) séparés du domaine principal (ex : adminprenom@admindomaine.fr), sans boîte email réelle (réduit l'exposition au phishing), avec FIDO2 comme seule méthode MFA autorisée

(Authentication Strength dans CA), et en eligible assignment PIM uniquement. Ces comptes admin dédiés ne doivent jamais être utilisés pour des tâches non-administratives (navigation web, email), réduisant drastiquement la surface d'exposition.



Les ressources officielles Microsoft pour le durcissement Entra ID et les meilleures pratiques de sécurité identité : la documentation "Microsoft Entra security operations guide" est disponible sur learn.microsoft.com. Le benchmark CIS Microsoft Entra ID, développé par le Center for Internet Security, est disponible gratuitement sur cisecurity.org — les deux références complémentaires et indispensables pour structurer un programme de durcissement Entra ID complet, répétable et aligné avec les standards industriels reconnus.