Le MFA ne suffit plus : il faut passer à une authentification réellement résistante au phishing

SÉCURITÉ DE L'IDENTITÉ | MICROSOFT 365 | ZERO TRUST

Le constat	Le problème	La réponse
Le MFA seul ne protège plus contre les attaques modernes sur la chaîne d'authentification.	Phishing avancé, vol de session, fatigue push, méthodes faibles et exceptions mal gérées.	Passer à une authentification forte, résistante au phishing, intégrée dans une stratégie globale.

Le MFA reste indispensable — mais il ne suffit plus

Pendant longtemps, le MFA a été présenté comme une protection presque incontournable contre les compromissions de comptes. Et c'est vrai : activer le MFA reste indispensable.

⚠ Mais aujourd'hui, le constat est clair : le MFA seul ne suffit plus.

Les attaquants ne cherchent plus uniquement à deviner un mot de passe. Ils ciblent désormais toute la chaîne d'authentification :

L'utilisateur

Manipulation sociale, phishing ciblé, fatigue push.

La session

Vol de token après authentification valide.

Le navigateur

Interception en temps réel via proxy adversarial.

Les jetons d'accès

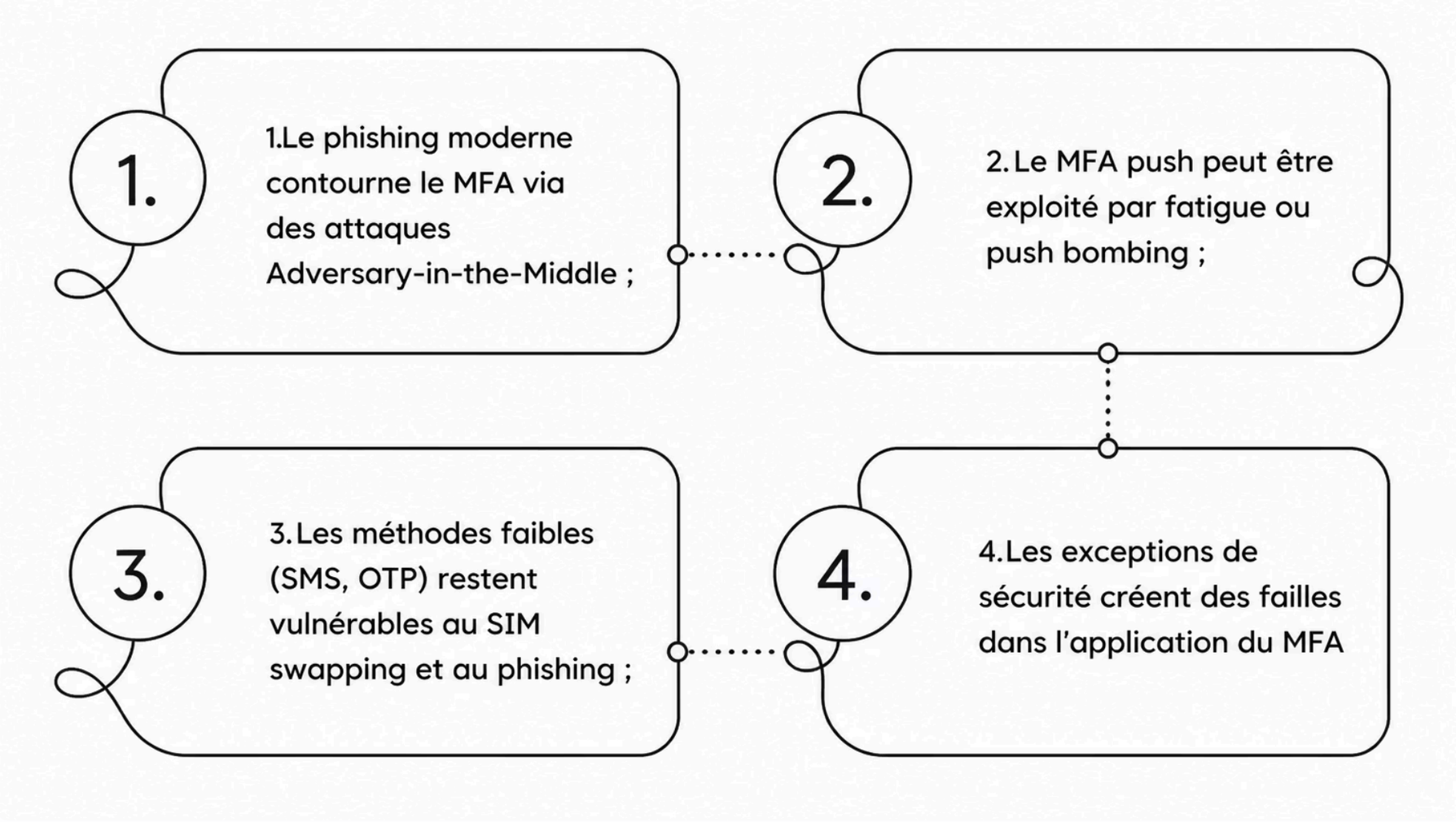
Réutilisation de tokens MFA-validés depuis une autre machine.

OAuth & exceptions

Applications OAuth, bypass MFA, Conditional Access mal configuré.

Pourquoi le MFA ne suffit plus ?

Quatre vecteurs d'attaque démontrent que le MFA classique présente des lacunes structurelles face aux menaces actuelles. Chacun de ces vecteurs exploite une faiblesse différente de la chaîne d'authentification.



Ces quatre vecteurs ne sont pas théoriques : ils sont activement exploités dans des campagnes ciblant les environnements Microsoft 365 et Azure AD.

1. Le phishing moderne contourne le MFA

Le mécanisme AiTM

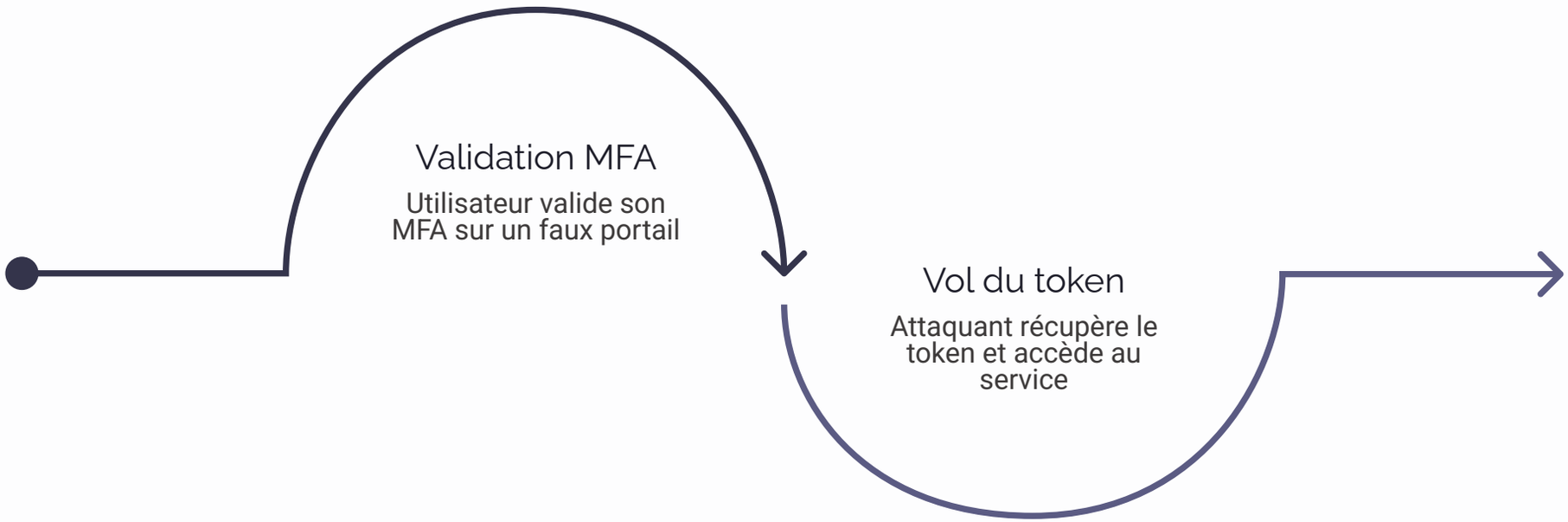
Les attaques de type **Adversary-in-the-Middle** peuvent intercepter une session après validation du MFA. L'utilisateur pense se connecter à un portail légitime, valide son MFA, mais l'attaquant récupère ensuite un jeton de session déjà authentifié.

Ce que dit Microsoft

Microsoft décrit ce scénario : après une connexion valide, un attaquant peut voler un **token de session MFA-validé** et l'utiliser depuis une autre machine.

Dans ce cas, le MFA a bien été validé, mais la session est quand même compromise.

⊗ Le MFA protège l'entrée — pas ce qui se passe après.



2. Le MFA push peut être exploité par fatigue

Les attaques de **MFA fatigue** ou **push bombing** consistent à envoyer plusieurs demandes d'approbation jusqu'à ce que l'utilisateur accepte par erreur, par lassitude ou par confusion.

Le déroulement de l'attaque

01

Compromission du mot de passe

L'attaquant obtient les identifiants via phishing ou fuite de données.

02

Bombardement de notifications push

Des dizaines de demandes d'approbation sont envoyées en rafale sur le téléphone de la victime.

03

Acceptation par erreur ou lassitude

L'utilisateur finit par approuver pour faire cesser les notifications.

La réponse de Microsoft

C'est pour cette raison que Microsoft insiste sur l'importance du **number matching** dans Microsoft Authenticator, afin d'éviter le simple bouton *"Approve"*.

> Le number matching oblige l'utilisateur à saisir un code affiché à l'écran, rendant l'approbation aveugle impossible.

3. Les méthodes faibles restent vulnérables

Tous les MFA ne se valent pas. Le SMS, l'appel téléphonique ou les OTP classiques peuvent être exposés à plusieurs risques.

Interception

Les SMS peuvent être interceptés via des attaques sur le protocole SS7 ou des équipements compromis.

SIM Swapping

L'attaquant convainc l'opérateur de transférer le numéro de téléphone vers une SIM qu'il contrôle.

Phishing en temps réel

L'OTP saisi sur une fausse page est immédiatement rejoué par l'attaquant sur le vrai site.

Réutilisation

Un code OTP intercepté peut être utilisé dans une attaque en temps réel avant son expiration.

> Le vrai sujet n'est donc plus seulement : *"Avons-nous du MFA ?"*
> La bonne question devient : *"Notre MFA est-il résistant au phishing ?"*

4. Les exceptions de sécurité créent des failles

Dans beaucoup d'environnements Microsoft 365, le problème ne vient pas uniquement de l'absence de MFA, mais de son **application partielle**.

Les failles de configuration courantes

- Comptes exclus temporairement
- Groupes de bypass MFA
- Trusted locations trop larges
- Comptes de service mal protégés
- Anciennes méthodes d'authentification
- Politiques Conditional Access en mode report-only
- Comptes administrateurs non séparés

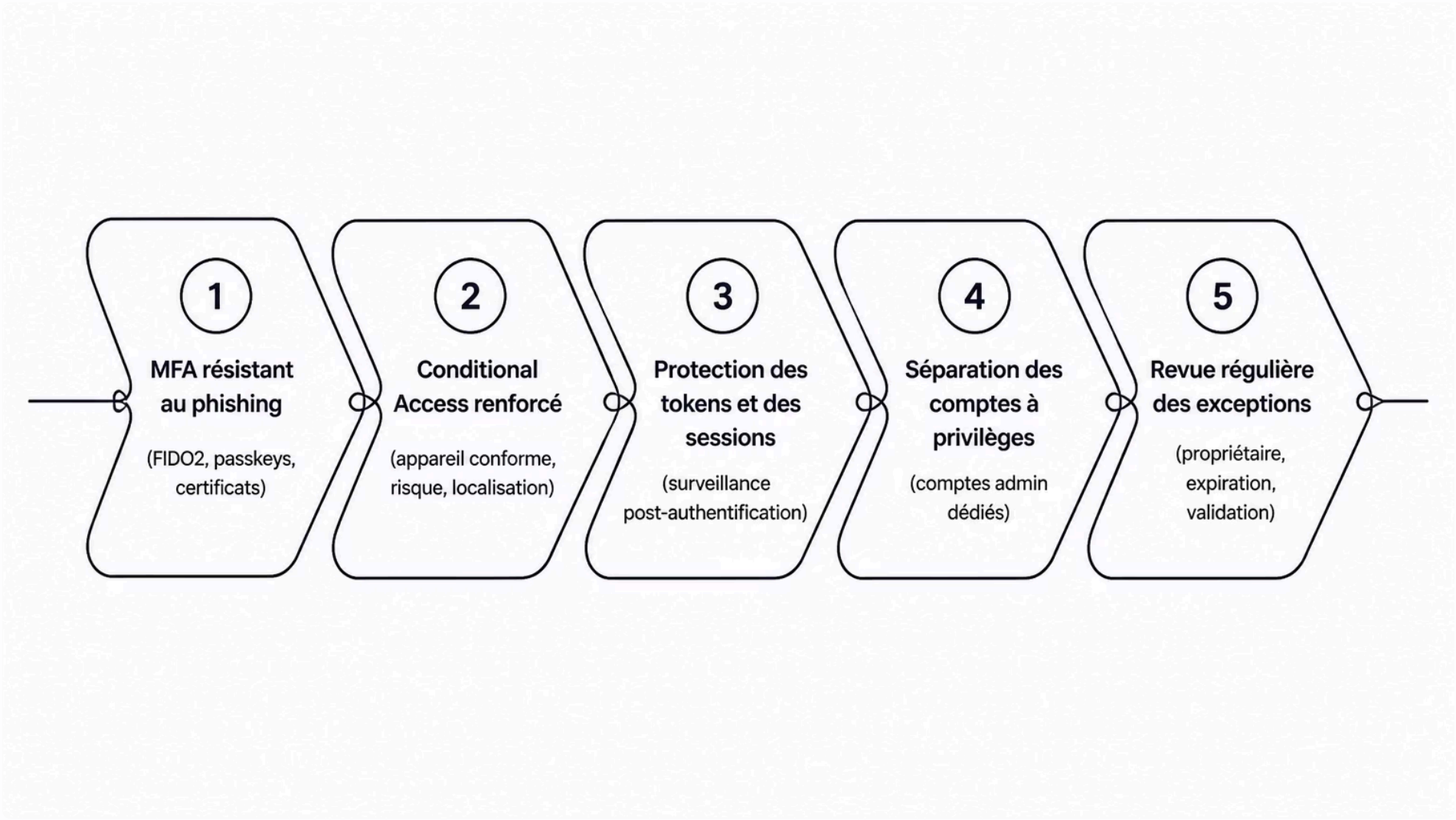
Cas réel : Microsoft 365

Une attaque récente contre Microsoft 365 a montré que des **millions de tentatives de connexion** pouvaient exploiter des faiblesses de configuration, notamment autour d'OAuth, de ROPC et de politiques MFA/Conditional Access insuffisamment appliquées.

Une exception temporaire devient souvent une faille permanente. Chaque exclusion du périmètre MFA est une surface d'attaque potentielle.

La solution : passer d'un MFA "classique" à une authentification forte

Le MFA reste nécessaire, mais il doit être intégré dans une stratégie plus globale.



Nécessaire mais insuffisant

MFA classique : SMS, OTP, push simple — protège l'entrée mais pas la session.

L'objectif cible

Authentification résistante au phishing : cryptographie, liaison au domaine, sans mot de passe.

La stratégie globale

MFA fort + Conditional Access + appareil conforme + protection des sessions + surveillance continue.

1. Déployer du MFA résistant au phishing

Les méthodes à privilégier sont celles qui reposent sur la cryptographie et sont liées au domaine légitime, rendant le rejeu impossible.

FIDO2 / Clés matérielles

YubiKey et équivalents. La clé physique est liée au domaine — impossible à phisher à distance. Standard recommandé par la CISA.

Passkeys

Authentification cryptographique sans mot de passe, liée à l'appareil et au domaine. Résistante aux attaques AiTM.

Windows Hello for Business

Authentification biométrique ou PIN liée à l'appareil et au tenant Azure AD. Déploiement natif dans les environnements Microsoft.

Authentification par certificat

Certificats clients liés à l'identité de l'utilisateur et à l'appareil. Niveau de confiance élevé pour les accès sensibles.

La CISA recommande explicitement la mise en place d'un MFA résistant au phishing, notamment via des mécanismes basés sur la cryptographie et liés au domaine légitime.

2. Renforcer Conditional Access

Le MFA doit être combiné avec des contrôles contextuels. Une politique Conditional Access robuste évalue le risque à chaque tentative de connexion, pas seulement à l'entrée.

Contrôles sur la connexion

- Bloquer les connexions à risque élevé
- Exiger un appareil conforme ou hybride joint
- Limiter les sessions persistantes
- Bloquer les protocoles legacy

Contrôles sur le contexte

- Contrôler les accès depuis pays ou IP inhabituels
- Imposer une authentification forte pour les administrateurs
- Surveiller les connexions impossibles ou anormales
- Réduire strictement les exceptions

⚠ Une politique Conditional Access en mode **report-only** ne protège pas. Elle doit être activée en mode **enforced** pour avoir un effet réel.

3. Protéger les tokens et les sessions

Le MFA protège l'entrée, mais il faut aussi protéger ce qui se passe après l'authentification. La surveillance des signaux post-connexion est essentielle pour détecter un vol de session.

1

Changement de localisation

Changement soudain de localisation géographique après une connexion valide.

2

Nouvel appareil

Token utilisé depuis un appareil non reconnu ou non enregistré.

3

Connexion sans interaction

Connexion réussie sans interaction utilisateur cohérente avec le comportement habituel.

4

Accès inhabituels

Accès inhabituel à SharePoint, Exchange, Teams ou OneDrive en dehors des patterns normaux.

5

Règles de transfert mail

Création suspecte de règles de transfert mail vers des adresses externes.

6

Consentement OAuth

Consentement OAuth non autorisé accordé à une application tierce.

4. Séparer les comptes à privilèges

Les comptes administrateurs doivent être traités différemment des comptes utilisateurs standards. La séparation des privilèges est un principe fondamental de la sécurité Zero Trust.

Principe de séparation

Un administrateur doit disposer de **deux comptes distincts** : un compte nominatif standard pour l'usage quotidien (email, Teams, navigation) et un compte administrateur séparé, utilisé uniquement pour les tâches d'administration.

Cette séparation limite drastiquement la surface d'attaque en cas de compromission du compte quotidien.

Exigences pour les comptes admin

MFA phishing-resistant obligatoire

FIDO2, certificat ou Windows Hello for Business — aucune exception.

Accès conditionnel renforcé

Appareil conforme, localisation contrôlée, session non persistante.

Aucune exception permanente

Toute dérogation doit être temporaire, justifiée et tracée.

Journalisation et revue régulière

Audit des connexions admin, revue des droits, alertes sur les anomalies.

5. Revoir régulièrement les exceptions

Une exception MFA temporaire devient souvent une faille permanente. La gestion rigoureuse du cycle de vie des exceptions est un élément critique de la posture de sécurité.

Un propriétaire

Chaque exception doit être rattachée à une personne responsable, nommément identifiée.

Une justification

La raison métier ou technique doit être documentée et validée formellement.

Une date d'expiration

Aucune exception ne doit être permanente par défaut. Une durée maximale doit être définie.

Une validation sécurité

L'équipe sécurité doit approuver chaque exception avant sa mise en place.

Une revue périodique

Les exceptions actives doivent être réévaluées régulièrement et supprimées dès que possible.

Sans processus formel de gestion des exceptions, chaque dérogation accordée est une porte potentiellement ouverte indéfiniment.

Conclusion

> Le MFA n'est pas mort. Mais le MFA "classique" n'est plus suffisant.

La sécurité moderne doit évoluer vers une approche plus robuste :

1

MFA fort

FIDO2, passkeys, certificats

2

Conditional Access

Contexte, risque, appareil conforme

3

Protection des sessions

Surveillance post-authentification

4

Surveillance continue

Détection des anomalies et réponse

L'objectif a changé

Aujourd'hui, l'objectif n'est plus simplement de demander un second facteur.

L'objectif est d'**empêcher qu'un attaquant puisse voler, rejouer ou contourner l'authentification**.

La prochaine étape

Le MFA est une base. La résistance au phishing est la prochaine étape.

Chaque organisation doit évaluer sa posture actuelle : quelles méthodes MFA sont déployées, quelles exceptions existent, quels comptes admin sont exposés, et quels signaux post-authentification sont surveillés.