IDENTITY DAYS

20 octobre 2026
PARIS

Passwordless sans baguette magique… tout ce qu’on oublie avant la prod

David Pollet & Hakim Taoussi

David Pollet

Practice Leader Cyber et associé Wakers, architecte sécurité & identité (AD, Entra ID, M365)

Hakim Taoussi

Cybersecurity Director chez IT Systemes, Microsoft MVP

Agenda de la conférence

- La promesse
- L’enrôlement initial
- La récupération d’accès
- Les applications héritées
- Au-delà d'Entra ID
- La surface des méthodes
- Le secret qui reste
- Le helpdesk
- Le programme transverse
- La roadmap
- Ce qu il faut retenir

La promesse

PROMESSE VS PRODUCTION

La promesse est simple.
La production ne l’est pas.

Le vrai projet commence là où la démo s’arrête.

La promesse

- Une méthode, tout le monde bascule
- Ça marche avec vos applications
- Les utilisateurs s’enrôlent seuls
- Plus de mots de passe
- Fini le phishing

La réalité

- Méthodes et variantes à gouverner
- Applications legacy, VPN et RDP à traiter
- Clés perdues, helpdesk dans le périmètre
- Le hash reste dans l’annuaire
- La session, elle, se vole

Question clé : sommes-nous prêts à absorber ces changements sans créer de contournement ?

CHAÎNE DE CONFIANCE

Passwordless n’est pas une méthode.

C’est une chaîne de confiance.

Chaque maillon peut réintroduire le mot de passe - ou devenir le chemin de moindre résistance.

1	2	3	4	5	6	7
Identité Qui est l’utilisateur?	**Enrôlement initial** première preuve	**Méthodes** WHfB, passkeys, certificat	**Device** conformité et état	**Applications** auth moderne ou passerelle	**Recovery** chemin de secours	**Operations** run, support, audit

Règle de conception : un utilisateur ne doit jamais être plus facile à récupérer qu’à authentifier.

Trois actes :
ce qui casse, ce qui reste exposé, ce qu'on opère.

ACTE I
Ce qui casse

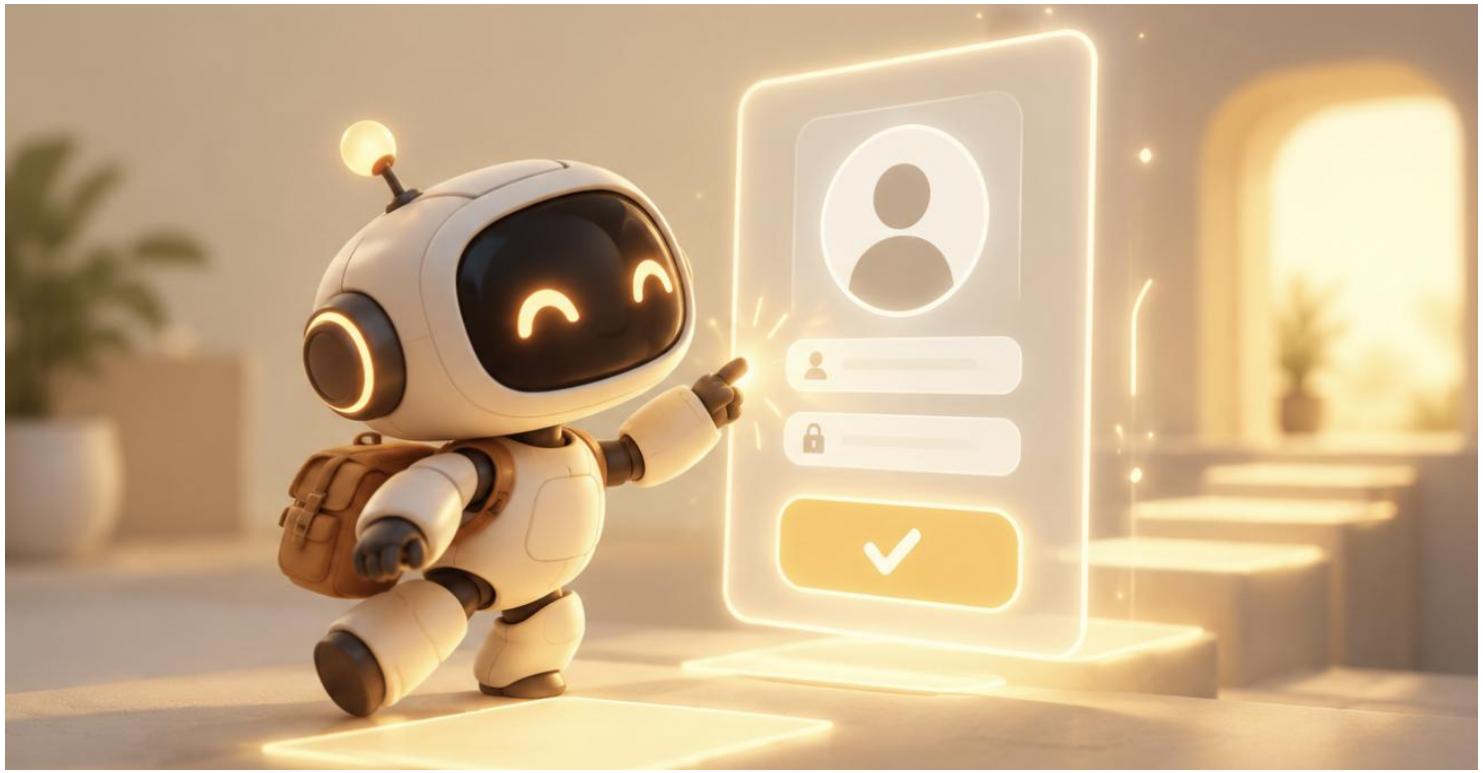
- Enrôlement initial
- Récupération d'accès
- Applications héritées
- Surfaces d'authentification
- Comptes de service
- Prérequis WHfB, RDP et VDI
- Méthodes faibles et secret AD

ACTE II
Ce que la méthode ne couvre pas

- Vol de session et de jeton
- Choix de la méthode
- Device-bound vs synced

ACTE III
Opérer et déployer

- Postes et terminaux partagés
- Helpdesk comme opérateur
- Programme transverse
- Architecture cible



L'enrôlement initial

BOOTSTRAP

ACTE I

L’enrôlement initial :

Créer le premier moyen d’authentification exige déjà de prouver son identité.

Avant de pouvoir s’authentifier sans mot de passe, il faut d’abord enregistrer un moyen d’authentification.

1. **Utilisateur sans moyen d’authentification**
2. **Preuve initiale**
3. **TAP court et contrôlé**
4. **Enrôlement WHfB, passkey, FIDO2**

Constat terrain

- TAP souvent transmis par un **canal non sécurisé**
- Un TAP satisfait la MFA Entra ID : c’est un **secret à forte valeur**

Contrôles

- PIM/JIT, usage unique, durée minimale
- Canal distinct, preuve d’identité, journalisation
- CA « Register security information » : **device conforme ou réseau de confiance exigé**

Décision à écrire

- Qui crée, valide, délivre ?
- Quelle durée, quel canal ?
- Et hors horaires ?

La récupération d'accès

RECOVERY

ACTE I

La récupération d’accès:
le vrai test n’est pas J0, c’est J+3.

« J’ai perdu ma clé et mon téléphone » : trois scénarios, trois niveaux de preuve.

A

2e méthode disponible

Auto-récupération contrôlée

L’utilisateur se ré-enrôle seul, sans ticket.

B

Toutes méthodes perdues

Ré-enrôlement assisté, identité vérifiée

Vérification renforcée avant toute délivrance.

C

Processus manuel

Helpdesk, preuve forte, TAP

Canal séparé , TAP court, geste tracé.

Objectif : aucune récupération basée uniquement sur la connaissance de données personnelles.

Les applications héritées

APPLICATIONS LEGACY

ACTE I

Les applications héritées: l'échec vient du dernier kilomètre.

Le Passwordless échoue rarement sur Microsoft 365. Il échoue sur ce qui reste autour.

VERT

Natif / moderne

Browser moderne, MSAL + broker, apps Microsoft à jour.

ORANGE

Compatible sous conditions

RDP / VDI, VPN à certificats, apps embarquant un browser.

ROUGE

Dépendance mot de passe

Protocoles anciens, RunAs, consoles, clients propriétaires.

Si vos utilisateurs utilisent Windows Hello for Business le matin, mais doivent encore saisir leur mot de passe dix fois dans la journée, êtes-vous réellement Passwordless ?

Au-delà d'Entra ID

SURFACES D'AUTHENTIFICATION

ACTE I

Passwordless dans Entra

≠ Passwordless partout.

Un même utilisateur traverse plusieurs plans d'authentification dans une journée.

SURFACE	CHEMIN CIBLE	STATUT
Windows logon	WHfB / clé FIDO2	**Très bon**
Apps SaaS / M365	Passkey / WHfB	**Très bon**
Ressources AD on-prem	Kerberos via WHfB / Cloud Kerberos Trust	**Bon si préparé**
VPN	Dépend du client et du protocole	**À qualifier**
RDP / VDI	Certificat WHfB ou Remote Credential Guard	**Faisable si outillé**
RunAs / console serveur	Certificat WHfB, hors UAC bureau sécurisé	**Limite documentée**

La suppression du mot de passe se pilote par surface, pas seulement par utilisateur.

COMPTES DE SERVICE

ACTE I

Les comptes de service : le passwordless humain ne les couvre pas.

Un même parc mélange identités humaines et identités machine, avec deux modèles de preuve différents.

Humains

- WHfB
- Passkeys
- FIDO2 security keys
- Certificate-Based Authentication

Non-humains

- Managed identities
- gMSA / dMSA
- Workload identities
- Certificats / clés
- Secrets à rotation (dev)

Authentification sans mot de passe des utilisateurs ≠ infrastructure sans secrets.

PRÉREQUIS WHfB

ACTE I

Les prérequis WHfB :
activer est facile, avoir le bon modèle moins.

Le vrai travail porte sur le modèle de confiance, pas sur l'activation.

MODÈLE	PRÉ-REQUIS	POINT D'ATTENTION
Cloud only	Entra joined	Le plus simple
Hybrid + Cloud Kerberos Trust	Entra / Hybrid joined	**Recommandé Microsoft**
Hybrid + Key Trust	Writeback sync +pki	msDS-KeyCredentialLink
Hybrid + Certificate Trust	PKI + certificats utilisateurs	Certificats, carte à puce

Le modèle recommandé n'est pas universel : RDP, VPN, certificats ou postes partagés changent la cible.

RDP, VDI ET ÉLÉVATION

ACTE I

RDP et RunAs

WHfB ne fournit pas un mot de passe délégable. Pour RDP, on utilise soit un certificat WHfB via la redirection smart card, soit Remote Credential Guard qui redirige les requêtes Kerberos vers le poste source.

OPTION	PRÉ-REQUIS	LIMITE
Certificat dans le conteneur WHfB	PKI, SCEP/PKCS ou AD CS	RunAs cassé (cert Intune)
Remote Credential Guard	Kerberos, hôte 2016+	Hôte cible AD-joined
AVD / Windows 365, auth Entra	Hôtes Entra ou hybrid joined	AD-only non supporté
Redirection WHfB / FIDO2	SSO Entra activé sur le pool	À valider par application

RCG : authentification Kerberos sans transmission des identifiants à l'hôte distant. RunAs : traitement spécifique des comptes privilégiés.

La surface des méthodes

SURFACE DES MÉTHODES

ACTE I

Ajouter du fort sans retirer le faible ne réduit rien.

Le risque reste celui du chemin le plus faible encore autorisé.

MÉTHODES ENCORE AUTORISÉES

Passkey	**WHfB**	**FIDO2**
TOTP	**Push**	**TAP**
SMS	**Voice**	**Password**

Vert : résistant au phishing
Jaune : phishable (ex. Authenticator phone sign-in)
Rouge : à retirer de la policy

.

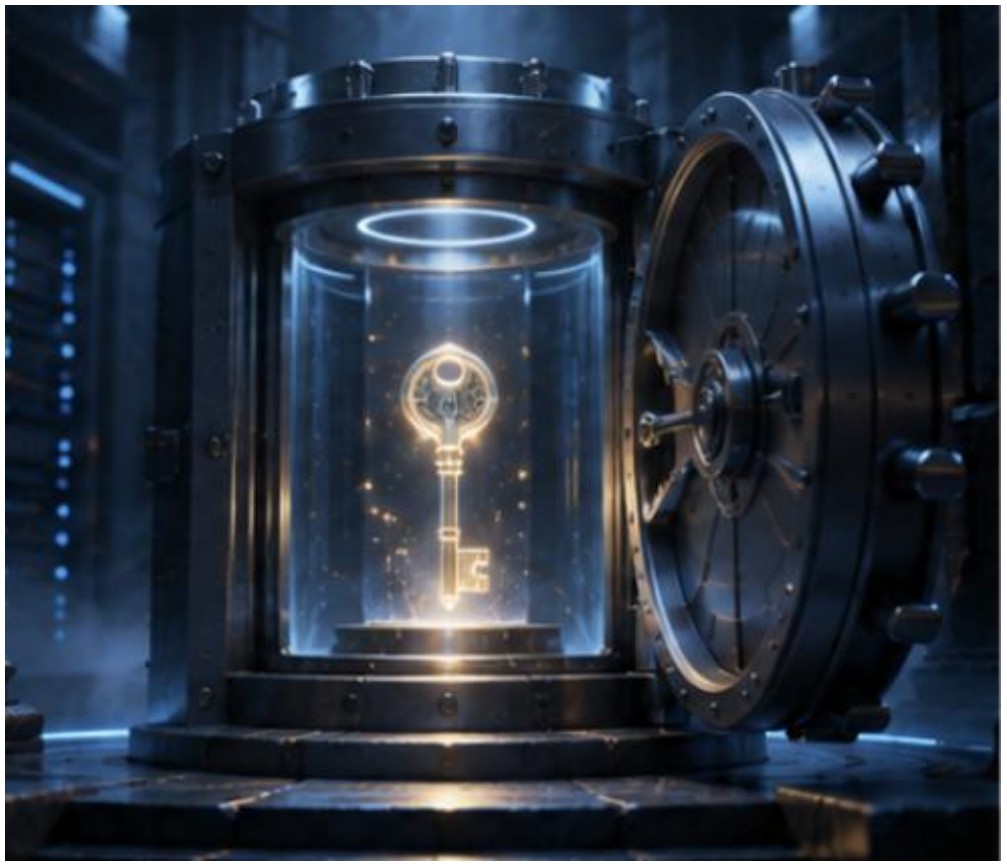
TROIS LEVIERS DE PILOTAGE

Authentication Methods Policy
Qui peut enregistrer et utiliser quelle méthode ?

Authentication Strength
Quelle assurance est obligatoire pour cette ressource ?

Conditional Access
Dans quel contexte cette assurance s'applique ?

Objectif : supprimer les fallbacks faibles quand les usages sont prêts - pas avant



Le secret qui reste

USAGE ≠ ANNUAIRE

ACTE I

Un utilisateur 100 % WHfB garde un secret exploitable dans AD.

Supprimer le mot de passe côté usage ne le supprime pas côté annuaire : le hash reste, et NTLM l'accepte.

LEVIER	EFFET	POINT D'ATTENTION
Carte à puce obligatoire (SCRIL)	Le secret est randomisé	NTLM et RunAs cassent
DFL Windows Server 2016 + msDS-ExpirePasswordsOnSmartCardOnlyAccounts activé	Rotation automatique du hash	Niveau fonctionnel requis
Réduction puis blocage de NTLM	Moins de chemins faibles	Auditer avant de bloquer
Comptes de secours hors SCRIL	Secours si la chaîne casse	Nombre limité, surveillé

Tant que le hash vit dans l'annuaire, le mot de passe reste un chemin d'attaque, même sans usage.

MODÈLE DE MENACE

ACTE II

La méthode résiste au phishing.
La session, elle, se vole.

AiTM, refresh token, device code flow, consentement : le vol de jeton contourne la méthode d'authentification.

CHEMIN	CONTRE-MESURE		PORTÉE
AiTM, vol de cookie	Device conforme Intune exigé en CA	🟢	Web et natif sur device géré
Vol de PRT / refresh token	Token protection : jeton lié au device	🟢	Selon matrice Microsoft
Device code flow	Blocage du flux en Conditional Access	🟢	Exceptions listées
Consentement OAuth	Consentement admin, revue des apps	🟠	Gouvernance continue
Contexte qui change	Évaluation continue d'accès (CAE)	🟠	Apps compatibles
Poste non géré	Filtre de device, durée de session	🟠	Selon la ressource
Plateforme hors périmètre	Bloquer les plateformes inconnues	🟠	Conformité sur les connues

le Passwordless protège l'authentification. Mais il faut aussi protéger ce qui se passe après : la session et les jetons.

CHOIX DE LA MÉTHODE

ACTE II

« Passkey »
n’est pas une seule décision.

Le compromis se joue entre provenance, portabilité, coût et récupération d’accès.

OPTION	TYPE	PERSONA	RISQUE
FIDO2 security key	Device-bound	Admins / régulé	Perte physique, stock
Passkey in Microsoft Authenticator	Device-bound	Utilisateurs mobiles	Dépendance mobile
Synced passkey	Synchronisée	Population large	Confiance au provider
WHfB / Windows passkey	Device-bound	Poste managé Windows	Dépend du device

il ne faut pas choisir une seule méthode pour toute l'entreprise, mais adapter le type de passkey au niveau de risque et aux usages de chaque population.

FRONTIÈRE DE CONFIANCE

ACTE II

Device-bound vs synced :
même résistance au phishing, pas la même frontière.

La clé privée ne vit pas au même endroit - et la confiance non plus.

Device-bound passkey

Utilisateur → authenticator physique → Entra ID

Clé privée sur un seul authenticator.

Synced passkey

Utilisateur → device → provider → autres devices

Le provider entre dans la chaîne de confiance.

Contrôle entreprise	AAGUID / attestation possibles	Dépend du provider, non attesté
Recovery utilisateur	Plus lourd, plus contrôlable	Plus simple, confiance déplacée
Cible naturelle	Admins, Tier 0, populations sensibles	Utilisateurs standards, adoption large

Passwordless ne supprime pas les décisions de confiance : il les déplace.

POSTES PARTAGÉS

ACTE III

Postes et terminaux partagés : un utilisateur = un device ne tient pas partout.

Frontline, kiosques et ateliers demandent un flux dédié, pas une exception improvisée.

CONTEXTE	DEVICE	MÉTHODE	STATUT
Bureau personnel	PC attribué	WHfB / passkey	**OK**
Frontline mobile	Android / iOS partagé	QR code + PIN (**1FA**), Shared Device Mode	**OK**
Kiosque / salle	Device partagé	Appli ou Windows fido2	**À cadrer**
Atelier / legacy	Terminal ancien	Exception temporaire + plan de sortie	**À cadrer**

Erreur classique : forcer WHfB partout, puis recréer des comptes génériques.

Le helpdesk

HELPDESK

ACTE III

Le support devient un opérateur de confiance.

Le support ne fait plus un reset : il restaure une chaîne de confiance.

CAS	PROCEDURE
Clé perdue	Vérifier l'identité → supprimer la méthode → TAP → ré-enrôler
PIN WHfB bloqué	réinitialisation du PIN, le verrouillage TPM et la perte du conteneur WHfB
Passkey orpheline	Nettoyer le local, puis supprimer et recréer côté Entra
Téléphone remplacé	Révoquer les sessions si nécessaire, rebind des méthodes
Admin privilégié	PIM/JIT
Incident suspect	Stopper le recovery standard → procédure IR

Chaque procédure définit : vérification d'identité, habilitations RBAC, actions autorisées, traçabilité et escalade.

Le programme transverse

PROGRAMME TRANSVERSE

ACTE III

Le Passwordless n’est pas un projet IAM : plusieurs équipes tiennent une partie de la chaîne.

Si IAM porte seul le projet, les dépendances apparaissent trop tard.

IAM
Méthodes, TAP, strengths, CA

Endpoint
WHfB, device trust, Intune

AD / PKI
Kerberos, DC, certificats

Network
VPN, NAC, proxies

Apps
MSAL, brokers, legacy

Helpdesk
Recovery, stock, runbooks

Security
Threat model, logs, IR

Un seul propriétaire du programme.
Plusieurs propriétaires des dépendances.

ARCHITECTURE CIBLE · RAPPEL DE LA CHAÎNE

ACTE III

Forte par défaut,
Accès de secours contrôlé sur tout le cycle de vie.

On ne sécurise pas une méthode : on sécurise le cycle de vie complet.

Forte par défaut

Méthodes résistantes au phishing imposées par Authentication Strength.

Mécanisme de secours contrôlé

Chaque chemin faible est nommé, limité dans le temps et journalisé.

Exception cadrée

Un propriétaire, un périmètre, une justification et une date de sortie.

Chaque exception a un propriétaire, un périmètre, une justification et une date de sortie.
Deux comptes de secours restent exclus des accès conditionnels, en coffre, testés chaque semestre.

La roadmap

ROADMAP

ACTE III

Cinq phases avec des critères de sortie, pas un big bang.

Chaque phase produit des livrables qui conditionnent la suivante.

1	**Inventorier**	Méthodes existantes, apps, VPN, RDP, personas, accès de secours actuel
2	**Designer**	Authenticators par persona, enrôlement, recovery, architecture WHfB
3	**Piloter**	Anneau 0 et anneau 1, runbooks, mesures, cas cassants
4	**Industrialiser**	Enrôlement, stocks de clés, helpdesk, automatisation
5	**Enforcer**	Authentication strengths, retrait des accès de secours faibles, exceptions, KPI

Le retrait des mots de passe est une conséquence de la maturité, pas le point de départ.

Ce qu'il faut retenir

CONCLUSION

Le Passwordless est prêt.
Votre organisation doit l'être aussi.

Les six messages à retenir.

- Traiter l'enrôlement initial comme une opération privilégiée.
- Concevoir la récupération d'accès avant le déploiement.
- Inventorier les flux qui exigent encore un secret réutilisable.
- Choisir la méthode d'authentification par profil et par usage.
- Réduire puis supprimer les solutions de secours faibles.
- Protéger la session et le secret dans l'annuaire.

Passwordless, c'est moins un bouton

qu'un modèle d'exploitation.

20 % technologie

80 % exploitation

Décisions de confiance

IDENTITY DAYS
@IdentityDays
#identitydays2026