L'authentification sans mot de passe, des arguments séduisants

L'authentification sans mot de passe renforce la sécurité au niveau des points d'accès tout en simplifiant le processus de connexion pour les utilisateurs. Pas étonnant, donc, que cette méthode d'authentification connaisse un tel engouement. Attaques par rejeu, tentatives de phishing, divulgations suite au piratage d'un serveur... Aucun mot de passe, aussi fort soit-il, n'est inviolable. Sans parler des combinaisons difficiles à mémoriser pour les utilisateurs. À l'heure où le modèle Zero Trust s'impose dans les entreprises, chaque demande d'accès est désormais soumise à vérification. En ce sens, la sécurité des accès devient un enjeu majeur pour protéger contre les attaques sans entraver les performances et la productivité des salariés. Avec l'authentification sans mot de passe, fini le casse-tête de la création et de la mémorisation de mots de passe : l'identité des utilisateurs est vérifiée par des méthodes de connexion plus sécurisées.

Windows Hello Entreprise : un modèle de confiance basé sur les certificats

Windows Hello Entreprise (WHfB) est une solution Microsoft d'authentification sans mot de passe qui consiste à vérifier la connexion des utilisateurs via une authentification multifacteur sur PC et appareils mobiles, notamment par biométrie ou code PIN.

Le modèle de confiance basé sur les certificats de WHfB fait appel à des certificats numériques reposant sur une infrastructure à clé publique (PKI, Public Key Infrastructure). L'authentification auprès du service Active Directory (AD) s'opère ainsi par le biais de certificats émis par une Autorité de certification (AC).

Le modèle de confiance par clé authentifie les utilisateurs auprès d'un AD à l'aide d'une clé et nécessite des certificats auto-signés.

Parmi les deux principaux modèles de confiance pris en charge par WHfB, à savoir le modèle par clé et le mo]

•