

Authentification sans mot de passe en santé

ArchCare, l'un des principaux réseaux de santé de New York, a adopté les tokens matériels Hideez Key pour renforcer la sécurité des données et simplifier l'accès du personnel aux systèmes cliniques et administratifs.

DÉFIS

Tout au long de 2024 et jusqu'en 2025, le secteur de la santé aux États-Unis est resté une cible majeure des cyberattaques, avec les coûts de violation de données les plus élevés. Selon [le HHS Breach Portal](#), le principal vecteur d'attaque repose sur le piratage via des identifiants volés, souvent obtenus par phishing, permettant un accès non autorisé aux ePHI.

[La règle de sécurité HIPAA](#) impose aux organisations de santé des mesures techniques pour contrôler l'accès logique et physique aux ePHI. Dans un environnement clinique au rythme soutenu, cela représente un défi opérationnel. Pour les soignants utilisant des postes partagés, la saisie répétée de mots de passe crée un compromis entre efficacité et sécurité. Chaque connexion prend du temps, tandis que les mots de passe restent risqués.

SOLUTION

ArchCare, l'un des principaux prestataires de soins de santé basés à New York, a déployé les **tokens Hideez Key** pour renforcer la sécurité, simplifier les workflows cliniques et réduire les coûts dans son réseau d'hôpitaux et d'établissements de soins de longue durée. Ce déploiement a permis des gains de temps et de coûts en remplaçant trois outils d'authentification distincts : LastPass, les tokens RSA et les cartes HID.

Le personnel clinique utilise désormais une seule Hideez Key, souvent portée sur un tour de cou ou un enrouleur de badge, pour accéder facilement aux postes de travail, aux systèmes EHR et à d'autres applications critiques, tout en garantissant la sécurité et la conformité HIPAA.

PRINCIPAUX AVANTAGES

- 

Programme pilote gratuit – Les organisations peuvent tester la solution avec un petit groupe avant un déploiement complet.
- 

Déploiement rapide et simple – Disponible en version cloud ou on-premises, avec inscription des utilisateurs en libre-service.
- 

Sécurité éprouvée – Certifiée FIDO2 et U2F, conforme aux exigences européennes telles que NIS2 et DORA.
- 

Intégration transparente – Compatible avec Active Directory local, Entra ID, les postes de travail distants et toutes les applications héritées.



Méthodes d'authentification :

- 

Connexion biométrique passkeys
- 

Application mobile et codes QR uniques
- 

Tokens matériels Hideez Key

PREMIERS PAS

[Réservez une démonstration](#) pour découvrir le système et lancer un pilote gratuit adapté à vos besoins.

Les établissements de santé peuvent bénéficier de conditions spécifiques pour les entreprises, de scénarios d'authentification personnalisés et d'un support technique dédié.

En savoir plus : hideez.com/