

Les avantages d'une authentification optimisée **Sécurité**

Posté par : JulieM

Publié le : 9/1/2023 13:00:00

Poussés par l'accroissement des menaces de cybersécurité, par les exigences accrues pour protéger les travailleurs, par l'introduction d'initiatives Zero Trust, et par l'évolution des attentes des utilisateurs en matière de performances technologiques, les organisations adoptent massivement de nouvelles stratégies en matière de sécurité des identités. Or, pour rationaliser les processus d'authentification, il est essentiel de chercher à atténuer les frictions lors des accès.

Selon Fabrice de Vesian, Channel Manager chez Yubico, la performance des entreprises dépend fondamentalement de la capacité de sa main-d'œuvre à accéder et à utiliser efficacement les ressources numériques :

« Les processus de gestion des identités et des accès qui ralentissent les utilisateurs sont la principale cause d'interruption du travail et de dégradation de la productivité. Ces dernières années, la majorité des organisations ont cherché à faire face aux cybermenaces croissantes et à se familiariser avec les stratégies Zero Trust, en adoptant des solutions perçues comme plus faciles à mettre en œuvre.

Le recours continu aux contrôles basés sur les mots de passe, ainsi que les solutions d'authentification à second facteur centrées sur les appareils mobiles (telles que les mots de passe à usage unique par SMS ou par e-mail et les notifications push), n'ont cependant fait qu'augmenter la friction lors des demandes d'accès. Au final, la productivité des travailleurs se retrouve inhibée et l'efficacité de la sécurité est réduite.

Une étude menée par Enterprise Management Associates (EMA) conclut ainsi que les solutions d'authentification optimisées offrent des avantages significatifs aux entreprises. Ces atouts, notamment apportés par les technologies sans mot de passe et l'authentification adaptative, comprennent :

Amélioration de la satisfaction des employés avec les approches d'authentification sans mot de passe, comparées à celles traditionnelles opérant avec des mots de passe ;

Capacité à attirer et à retenir des employés talentueux. Parmi les travailleurs interrogés, 11 % ont déclaré qu'ils changeraient d'emploi s'ils devaient effectuer des tâches d'authentification contraignantes, et 53 % ont indiqué que la disponibilité de l'authentification sans mot de passe est une incitation importante pour les employeurs potentiels ;

Efficacité accrue de la sécurité. Les organisations prenant en charge l'authentification sans mot de passe et adaptative ont fait état de la plus grande confiance dans leur capacité à sécuriser les actifs IT de l'entreprise :

Gestion informatique simplifiée. L'authentification adaptative réduit les demandes d'assistance liées à l'identité de 39 %, tandis que les solutions sans mot de passe réduisent les volumes de tickets de 82 % ;

Coûts opérationnels réduits. Les entreprises ayant adopté des solutions d'authentification sans mot de passe sont nombreuses à déclarer avoir réalisé des

Économies de coûts quantifiables depuis le déploiement de ces solutions.

Les avantages apportés par les solutions d'accès optimisées sont donc indéniables. Avec 71 % des organisations citant la nécessité d'améliorer l'expérience de la main-d'œuvre et la productivité comme une priorité commerciale absolue, une adoption encore plus large de solutions d'accès à faible friction semble inévitable à l'avenir.

Cependant, les organisations ont parfois du mal à déterminer quelles approches répondront le mieux à leurs exigences organisationnelles uniques. »