yubico

Sécurité proactive pour les utilisateurs privilégiés

Développer des services financiers cyber-résilients

Tous les utilisateurs privilégiés d'une entreprise devraient bénéficier d'une sécurité maximale, mais de nombreuses entreprises ne protègent pas suffisamment leurs utilisateurs privilégiés et leur activité face aux attaques. Forrester estime qu'environ 80 % des brèches de sécurité impliquent des informations d'identification privilégiées[1], et selon Gartner, 56 % des responsables IT en entreprise ont tenté de déployer une solution de gestion des accès privilégiés (PAM), mais n'ont pas atteint leurs objectifs[2]. Les cybermenaces sophistiquées actuelles, alimentées par l'intelligence artificielle, peuvent facilement exploiter les utilisateurs et accéder à des systèmes ou données stratégiques si les utilisateurs privilégiés et leurs identifiants privilégiés sont compromis.

Vous avez peut-être plus d'utilisateurs privilégiés que vous ne le pensez

Les utilisateurs privilégiés étaient autrefois associés aux rôles d'administration IT et réseau. Cependant, les utilisateurs privilégiés correspondent en réalité à tous les utilisateurs qui opèrent à un niveau supérieur sur le réseau, le cloud ou les applications, avec un large accès aux systèmes exploitables, aux éléments de propriété intellectuelle ou aux informations personnelles identifiables et aux données financières des clients. Il peut s'agir de vos cadres supérieurs, des RH, des employés de banque, des employés de centre d'appels et d'autres collaborateurs de l'entreprise.

Les solutions IAM et PAM créent des angles morts de sécurité

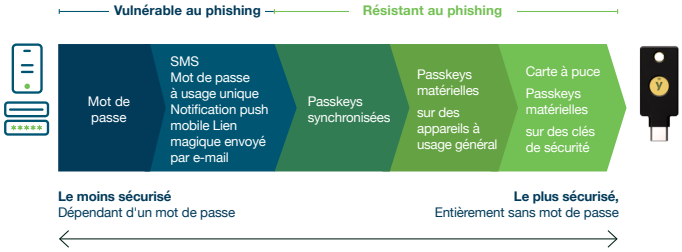
Pour renforcer leur positionnement en matière de sécurité, les organisations financières doivent déployer la gestion des identités et des accès (IAM) et la gestion des accès privilégiés (PAM). Les solutions IAM et PAM jouent un rôle considérable pour garantir aux bons utilisateurs les droits d'accès aux applications et aux données dont ils ont besoin. Cependant, elles laissent toujours des angles morts en matière de sécurité que les cybercriminels peuvent facilement exploiter. En voici quelques exemples :

- Peu de différenciation entre les droits d'accès et les droits privilégiés
- Intégration de l'accès privilégié avec le Single Sign-on (SSO) sans déploiement de l'authentification forte
- Absence de gestion des comptes privilégiés liés aux fournisseurs, aux employés temporaires ou aux anciens employés, ou même des comptes créés hors du contrôle de l'équipe IT (Shadow IT)
- Partage des informations d'identification et méthodes d'authentification classiques pour les comptes administrateur

Ces failles surviennent parce que la plupart des solutions de contrôle des accès classiques n'ont pas été conçues pour gérer des privilèges. Les entreprises doivent suivre le concept du moindre privilège, suivant lequel les utilisateurs ont différents niveaux de privilège en fonction de ce qu'ils doivent voir et faire au sein d'un système, en fournissant le moins d'accès possible (qui a accès à quoi) et le moins de privilèges possible (actions que quelqu'un peut entreprendre) associés à cet accès. Une solution PAM permet d'ajouter une couche de sécurité supplémentaire en séparant les privilèges des comptes utilisateur de ceux des comptes administrateur. Les dégâts seront ainsi limités si l'identité d'un utilisateur venait à être compromise. Les informations d'identification privilégiées doivent être archivées et extraites pour être utilisées, mais ces systèmes dépendent généralement de l'IAM pour l'authentification, ce qui nécessite souvent rien de plus qu'un mot de passe ou une authentification multi-facteurs (MFA) classique.

Le MFA classique met encore plus en danger les utilisateurs privilégiés

L'authentification classique, comme les noms d'utilisateur et les mots de passe, ainsi que les méthodes d'authentification mobile telles que les SMS, les mot de passe à usage unique et les notifications push, sont tous vulnérables au phishing et au piratage de compte. Lorsque ces attaques ciblent des comptes privilégiés, le risque de brèche et de ransomware augmente de manière exponentielle. Pour protéger les comptes des utilisateurs privilégiés et des administrateurs, toutes les entreprises de services financiers devraient déployer des passkeys modernes et résistantes au phishing dans toute l'entreprise, car en cas de brèche, chaque utilisateur est un utilisateur privilégié.

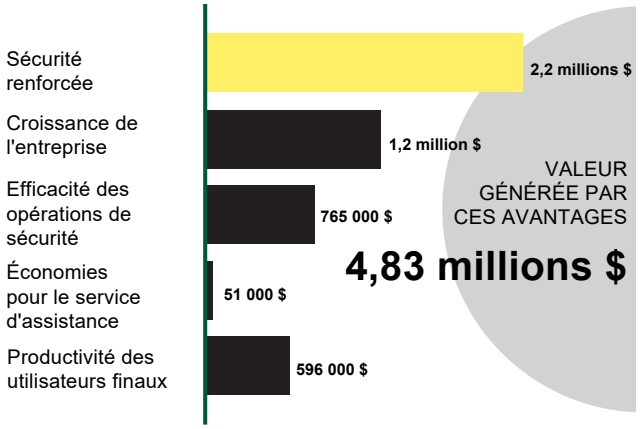


Déployez une sécurité proactive avec la YubiKey

Les YubiKeys sont des passkeys matérielles, la forme de passkey la plus sécurisée. Elles sont également portables, ce qui permet aux utilisateurs de travailler sur plusieurs appareils, notamment des postes de travail partagés, des tablettes et des appareils portables, qu'on retrouve communément dans les centres d'appels de services financiers et les sites de vente au détail.

Des chercheurs indépendants ont démontré que les YubiKeys constituaient la seule solution empêchant 100 % des piratages de comptes, y compris les attaques par phishing en masse et ciblées[3]. Elles génèrent également un retour sur investissement total de 203 % et une réduction de 75 % des tickets d'assistance liés aux mots de passe[4]. Pour s'authentifier à l'aide de la YubiKey, les utilisateurs se connectent d'un simple appui ou contact, ce qui augmente la productivité et offre la meilleure expérience et la plus grande conformité réglementaire pour les rôles en contact direct avec les clients.

YubiKey en chiffres



La YubiKey prend en charge les protocoles d'authentification modernes comme FIDO U2F et FIDO, ainsi que les OTP, les cartes à puce et OpenPGP, garantissant qu'une seule clé peut fonctionner pour l'ensemble des infrastructures et applications classiques et modernes et facilitant la transition vers un avenir sans mot de passe.

Les YubiKeys sont prêtes à l'emploi avec les solutions phares IAM et PAM et s'intègrent à des dizaines de systèmes tiers, notamment Hypr, Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, RSA SecurID Suite et CyberArk.

Les utilisateurs privilégiés détiennent les clés de toutes les entreprises, des clés que les cybercriminels sont prêts à tout pour obtenir. Déployez une authentification résistante au phishing pour protéger les utilisateurs privilégiés et votre entreprise contre les cybermenaces modernes.

Pour débuter, c'est très simple

N'exposez pas vos utilisateurs et votre entreprise au risque de piratage. Utilisez les YubiKeys dès maintenant !

Pour faciliter le déploiement d'une authentification résistante au phishing à grande échelle à l'aide de passkeys matérielles, Yubico propose YubiKey as a Service et YubiEnterprise Delivery pour faciliter l'approvisionnement et la livraison de YubiKeys.

- YubiKey as a Service offre aux entreprises un modèle de service abordable pour l'acquisition de YubiKeys, adapté à leurs besoins technologiques et contraintes budgétaires. Ce service offre également un support client prioritaire, une facilité de sélection du format, des remises sur les clés de sauvegarde et des avantages en matière de stock de remplacement.
- YubiEnterprise Delivery est un service cloud professionnel qui simplifie la distribution de YubiKeys aux utilisateurs finaux, desservant à la fois les sites nationaux et internationaux, y compris des adresses résidentielles.
- Yubico propose également Yubico Enrollment Suite, qui offre une expérience complète pour faciliter l'enregistrement des YubiKeys pour le compte des utilisateurs, actuellement compatible avec Microsoft et Okta, et bientôt avec d'autres fournisseurs d'identité (IdP).

YubiKey 5 Series, de gauche à droite : YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano et YubiKey 5C Nano.

Contactez-nous
yubi.co/contact

En savoir plus
yubi.co/finance

Yubico (Nasdaq Stockholm : YUBICO) est une entreprise de cybersécurité moderne dont la mission est de rendre Internet plus sûr pour tout le monde. En tant qu'inventeurs de la YubiKey, nous avons établi la norme d'excellence en matière de connexion simple et sécurisée, en empêchant les piratages de compte grâce à une authentification matérielle résistante au phishing.

Notre technologie protège des individus dans plus de 160 pays, offrant un accès rapide et sans mot de passe. Avec un double siège à Stockholm et Santa Clara, nous sommes convaincus que la sécurité renforcée doit être accessible à tous. Pour en savoir plus, rendez-vous sur www.yubico.com.