yubico

La MFA pour vos employés au bureau et à distance

Cinq étapes pour optimiser votre sécurité et votre productivité

Le travail hybride et à distance est désormais bien établi. Toutefois, l'adaptation à la nature flexible de ces environnements de travail peuvent poser des problèmes en matière de sécurité informatique, d'où l'urgence de faire preuve d'agilité et d'accueillir la transformation numérique. Les employés étant géographiquement dispersés, le périmètre de sécurité traditionnel et les formes d'authentification héritées (noms d'utilisateur, mots de passe et les authentificateurs mobiles) n'offrent plus une protection adéquate des accès aux réseaux, aux applications et aux données. Les noms d'utilisateur et les mots de passe peuvent facilement être compromis, et les authentificateurs mobiles sont vulnérables aux hameçonnages, aux programmes malveillants, aux SIM Swap, et aux attaques "man in the middle".

Protégez vos employés contre les menaces informatiques modernes grâce à la YubiKey, la clé de sécurité matérielle multi-protocole de Yubico qui fournit une authentification à deux facteurs (2FA), multi-facteurs (MFA) et sans mot de passe. La YubiKey est fournie sous plusieurs formats et offre une expérience utilisateur simple et mobile sur les ordinateurs de bureau, les ordinateurs portables, les appareils mobiles et les tablettes. La YubiKey permet également de réinitialiser soi-même les mots de passe, réduisant ainsi considérablement les coûts liés au support informatique. Des entreprises du monde entier procurent des YubiKey à leurs employés afin de garantir un accès sécurisé aux réseaux, aux données et aux applications de l'entreprise ainsi que pour réduire les coûts d'exploitation.

Suivez ces cinq étapes pour protéger vos employés, votre réseau et vos appareils grâce à la YubiKey :

1 Offrez un accès MFA aux systèmes de gestion des identités et des accès (IAM) et aux fournisseurs d'identité

La plupart des environnements hybrides et cloud exploite des solutions IAM pour permettre aux employés de travailler sans avoir à se compliquer la tâche avec plusieurs noms d'utilisateur et mots de passe selon les applications et les services de l'entreprise. La mise en place de la MFA sur votre plateforme IAM renforcera votre approche en matière de sécurité.

Renforcez la sécurité de l'ensemble de votre entreprise en adoptant la MFA avec la YubiKey. Les grandes plateformes IAM telles que Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, OneLogin, la plateforme Ping Identity et la suite RSA SecurID® prennent en charge les YubiKey et peuvent être utilisées pour l'authentification unique (SSO, Single Sign-on) pour les applications de messagerie et vidéoconférence telles que Microsoft Teams, Google Hangouts et Zoom.

2 Ne dépendez plus de l'authentification sur les appareils mobiles pour vous protéger des piratages de comptes

Les méthodes d'authentification en deux étapes telles que les codes secrets à usage unique et les notifications sont liées aux appareils mobiles. Or, ceux-ci sont susceptibles d'être compromis par un logiciel malveillant, un SIM Swap ou des attaques "man in the middle". Une étude, réalisée par Google, l'université de New-York et l'université de Californie à San Diego, basée sur 350 000 tentatives de piratage réelles, a démontré que les authentificateurs par SMS et appareils mobiles s'avèrent ne pas être une protection efficace contre le piratage de comptes et les attaques ciblées.[1]

Les intégrations YubiKey qui contribuent à sécuriser vos employés

DUO · FORGEROCK · idaptive · intercede · Microsoft · okta · ONE IDENTITY · onelogin · Onion ID · PingIdentity · secure W2

[1] Google Security Blog: New research: How effective is basic account hygiene at preventing hijacking

Protégez vos employés contre le piratage de comptes en remplaçant les authentificateurs mobiles par la YubiKey. En utilisant les normes d'authentification ouvertes modernes FIDO2 et WebAuthn, vous pouvez garantir le niveau de sécurité le plus élevé pour protéger vos employés contre l'hameçonnage et les attaques "man in the middle".

3 Sécurisez les technologies d'accès à distance

De nombreuses entreprises utilisent des réseaux privés virtuels (VPN) ou Identity-Aware Proxy (IAP) pour accéder à leurs réseaux, à des ressources protégées ou à des applications spécifiques. La connexion à un VPN ou à un IAP fournit une sécurité une fois la connexion établie. En revanche, une connexion WiFi privée ou publique non sécurisée demeure risquée si le VPN ou l'IAP est protégé par d'anciennes formes d'authentification.

La YubiKey assure la sécurité des accès à distance au moyen d'une authentification 2FA ou MFA pour les principales applications VPN telles que Pulse Secure et Cisco AnyConnect, ainsi que d'autres applications d'accès à distance, en s'appuyant sur les fonctionnalités Smart Card (PIV), mot de passe à usage unique (OTP), FIDO U2F ou FIDO2.

4 Protégez l'accès aux postes de travail

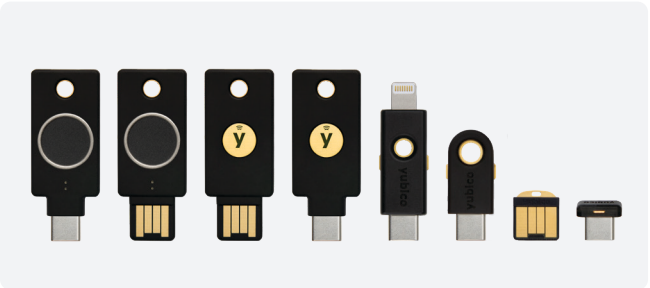
Si les ordinateurs portables de vos employés ne sont pas correctement protégés, ils peuvent offrir un accès aux menaces extérieures, créant ainsi une faille de sécurité pouvant entraîner des conséquences financières et juridiques, et porter préjudice à la réputation de votre entreprise.

Les YubiKey sécurisent la connexion aux ordinateurs en protégeant les applications et les données essentielles d'une entreprise. Plusieurs options de connexion incluent l'authentification pour les ordinateurs Mac et Windows, notamment ceux connectés via Azure Active Directory, Active Directory et les comptes Microsoft. L'utilisation de la fonctionnalité Smart Card de YubiKey, nécessitant une YubiKey et un code PIN, constitue l'un des moyens les plus efficaces de protéger l'accès à un ordinateur.

5 Adoptez une meilleure authentification pour les gestionnaires de mots de passe

De nombreux employés ont recours à un gestionnaire de mots de passe. Cependant, s'il n'est pas sécurisé grâce à une MFA anti-hameçonnage, ce gestionnaire est vulnérable aux attaques, offrant aux pirates un référentiel de mots de passe pour toutes vos applications et données d'entreprise.

La YubiKey s'intègre à plusieurs gestionnaires de mots de passe en entreprise, notamment 1Password, Dashlane, Keeper Security, LastPass et bien d'autres, veillant ainsi à ce que des politiques de gestion de mots de passe laxistes n'entraînent pas des failles sécuritaires.



Déployez dès aujourd'hui et en toute simplicité les YubiKey auprès de vos employés

Yubico offre des plans d'entreprise flexibles et rentables qui aident les organisations de 500 utilisateurs ou plus à s'éloigner des anciennes méthodes MFA et à se diriger vers une authentification résistante au phishing à grande échelle.

Avec YubiEnterprise Subscription, les entreprises peuvent bénéficier d'un modèle OPEX prévisible, de la flexibilité nécessaire pour répondre aux préférences des utilisateurs en choisissant n'importe quelle YubiKey, de mises à niveau vers les derniers modèles de YubiKeys et d'un déploiement plus rapide grâce à un accès facile aux services de déploiement et à l'assistance prioritaire. Les clients qui souscrivent cet abonnement peuvent également acheter des services et des offres de produits supplémentaires.

Contactez l'équipe de vente de Yubico dès aujourd'hui.

Les YubiKeys sont déployées dans :

- **9 des 10 plus grandes** entreprises de technolgie au monde
- **4 des 10 plus grandes** banques américaines
- **5 des 10 plus grands** détaillants au monde

À propos de Yubico Inventeur de la YubiKey, Yubico rend les connexions sécurisées faciles. Leader dans l'établissement de normes mondiales pour un accès sécurisé aux postes de travail et appareils mobiles, Yubico est le créateur et l'un des principaux contributeurs aux normes d'authentification ouvertes FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F). Pour plus d'informations, consultez : www.yubico.com.

Yubico AB
Kungsgatan 44
2ème étage
SE-111 35 Stockholm
Suède

Yubico Inc.
5201 Great American Pkwy
Suite 122
Santa Clara, CA 95054
États-Unis