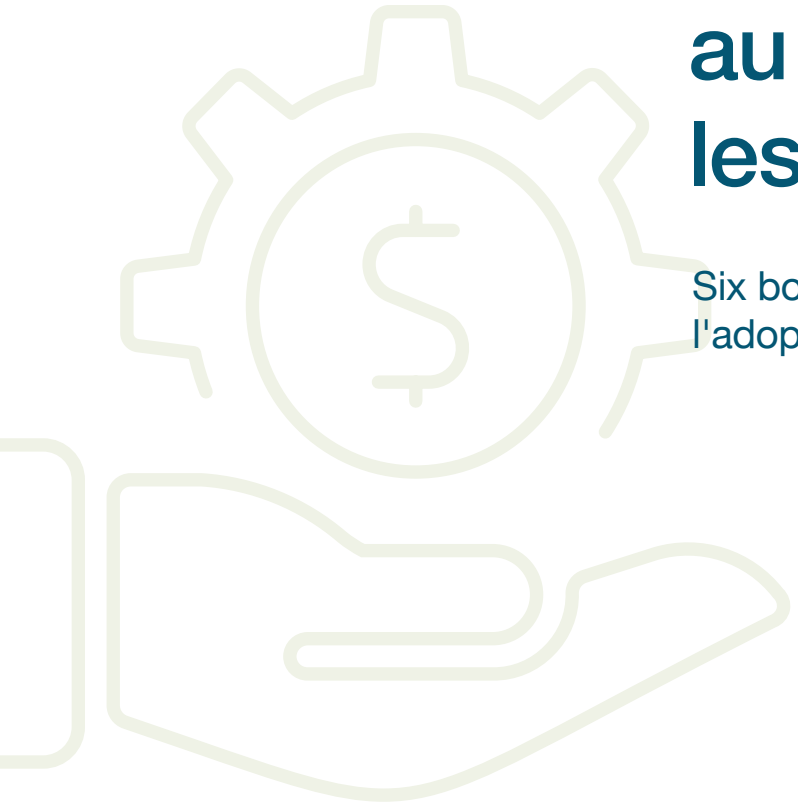
yubico

GUIDE DES BONNES PRATIQUES

Comment faire ses premiers pas avec le MFA résistant au phishing pour sécuriser les services financiers

Six bonnes pratiques de déploiement pour accélérer l'adoption à grande échelle



5,56 millions de dollars

coût moyen des brèches de données dans les services financiers[1]

82 %

des cybermenaces peuvent être attribuées à des informations d'identification volées[2]

D'après la publication spéciale (SP) 800-64 du NIST, seuls deux types d'authentification satisfont actuellement aux exigences d'un MFA résistant au phishing : **les cartes à puce/PIV** et le standard d'authentification moderne **FIDO2/WebAuthn**.

Choisir la bonne approche de MFA pour les services financiers

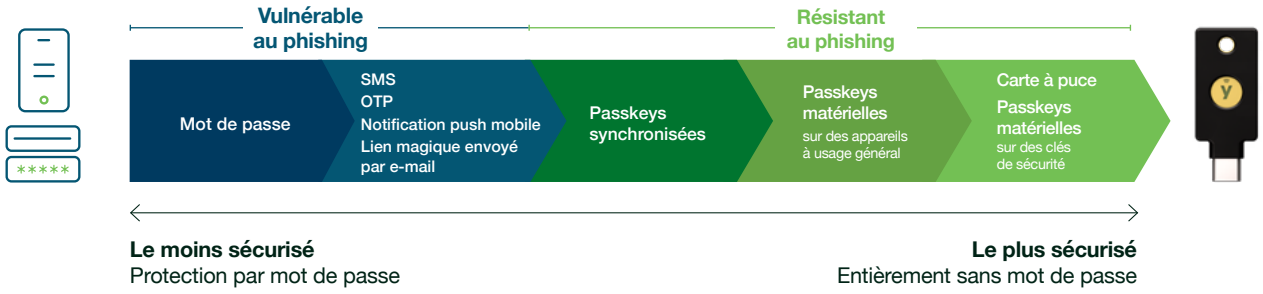
Les organisations financières sont confrontées à une pression croissante pour renforcer l'authentification face aux cybermenaces. En plus d'être coûteuses (le coût moyen d'une brèche de données s'élève à 5,56 millions de dollars américains[1]) et de saper la confiance des consommateurs, la majorité (82 %) des cybermenaces est liée à des informations d'identification volées. Il est donc logique que les organisations financières cherchent à renforcer les défenses de cybersécurité grâce à l'authentification multi-facteurs (MFA) et que les organismes de réglementation et les cyber-assureurs imposent également l'utilisation du MFA.

En 2021, la Federal Trade Commission (FTC) a modifié la « Safeguards Rule » (16 CFR 314)[3] de la loi Gramm-Leach-Bliley (GLBA), afin d'exiger l'utilisation du MFA pour les employés, les tiers et les clients. Cette règle a contribué à aligner les réglementations financières américaines sur les exigences européennes en matière de MFA, telles que définies dans la deuxième directive européenne sur les services de paiement (PSD2) et le règlement eIDAS (Identification électronique, Authentification et Services de Confiance).[4] En 2022, une circulaire du Consumer Financial Protection Bureau (CFPB) a précisé que l'absence de MFA pouvait entraîner une responsabilité au titre des réglementations du CFPB et de la loi Dodd-Frank, même en l'absence de brèche de données.[5] Tous ces éléments soulignent l'obligation d'adopter le MFA dans une démarche d'abandon des mots de passe peu sécurisés, sans toutefois indiquer quelle forme de MFA privilégier.

Aujourd'hui, l'environnement réglementaire commence à reconnaître que **toutes les formes de MFA ne se valent pas.** La plupart des méthodes d'authentification de base, telles que les SMS, l'authentification mobile et les mots de passe à usage unique, sont vulnérables aux piratages de comptes par phishing, par ingénierie sociale et de type « attacker-in-the-middle ». Conscients de ces vulnérabilités, les auteurs de la version révisée de la norme Payment Card Industry Data Security Standard (PCI DSS v4.0) ont introduit une norme financière sans précédent : le **MFA résistant au phishing** pour tout accès à l'environnement de données des titulaires de carte.[6]

Qu'est-ce que le MFA résistant au phishing ?

Les processus de **MFA résistant au phishing** reposent sur la vérification cryptographique entre des appareils ou entre un appareil et un domaine, ce qui les immunise contre les attaques qui tentent de compromettre ou de perturber le processus d'authentification.



La YubiKey protège 8 des 10 plus grandes banques mondiales

La YubiKey propose un MFA résistant au phishing

La YubiKey contient les passkeys les plus fiables, offrant une authentification multi-facteurs résistante au phishing ainsi qu'une authentification sans mot de passe. Contrairement à d'autres passkeys, celles-ci sont immunisées contre les compromissions, offrent une authentification portable et facile à utiliser, et sont générées et stockées de manière sécurisée dans un format matériel. Les YubiKeys prennent en charge plusieurs protocoles sur une seule clé, s'intègrent parfaitement aux environnements anciens comme modernes, et aident les organisations financières à **faire la transition vers un avenir sans mot de passe.** Les YubiKeys fonctionnent avec des centaines de produits, services et applications, y compris les principales plateformes de gestion des identités et des accès (IAM), les principales solutions de gestion des accès privilégiés (PAM) et des centaines de services de cloud.

Les clés de sécurité matérielles comme la YubiKey représentent une solution idéale pour un MFA résistant au phishing, car elles ne nécessitent ni alimentation externe, ni batterie, ni connexion réseau. Un utilisateur peut sécuriser des centaines d'applications et de services avec une seule clé, les secrets n'étant jamais partagés entre les services. La YubiKey a démontré sa capacité à réduire les risques de 99,9 %, tout en offrant une excellente expérience utilisateur, car elle permet une connexion sécurisée par simple pression ou contact.

Sécurité renforcée
Diminution des risques de 99,9 %

Rendement élevé
Retour sur investissement de 203 %

Plus de valeur
Réduction du nombre de tickets d'assistance de 75 %

Plus rapide
Authentification 4 fois plus rapide

Qu'en est-il des passkeys ?

Le terme « passkey » est une nouveauté dans le secteur, mais le concept lui-même n'a rien de nouveau. Les passkeys sont simplement des informations d'identification FIDO compatibles avec l'authentification sans mot de passe, permettant de s'affranchir des mots de passe tout en offrant une résistance au phishing.
Il existe différents modes de mise en œuvre des passkeys :

- **Les passkeys synchronisées** sont disponibles sur un smartphone, une tablette ou un ordinateur portable et peuvent être copiées d'un appareil à l'autre. Si les passkeys synchronisées facilitent la récupération des comptes en cas de perte ou de vol d'un téléphone ou d'un ordinateur portable, les informations d'identification FIDO sont quant à elles plus difficiles à retracer. Elles sont donc adaptées à des contextes ne nécessitant pas une sécurité extrêmement élevée.
- **Les passkeys matérielles** existent uniquement sur une clé matérielle spécialement conçue pour la sécurité, par exemple une YubiKey, adaptée aux niveaux les plus élevés de sécurité d'authentification et d'assurance de conformité.

Face à l'évolution des menaces, la nécessité d'un MFA résistant au phishing moderne est de plus en plus évidente. **Mais comment démarrer cette transition ?**

Six bonnes pratiques essentielles pour accélérer l'adoption du MFA résistant au phishing

Pour débuter, c'est très simple. Fort de son expérience pour le déploiement d'un MFA résistant au phishing auprès de centaines de clients, dont 4 des 10 plus grandes banques américaines, Yubico a élaboré un processus de déploiement en six étapes pour planifier et accélérer l'adoption du MFA résistant au phishing à grande échelle.

Planification

Assurez la préparation et l'alignement avant l'exécution

Validation

Validez le processus auprès d'un petit groupe d'utilisateurs avant un déploiement plus large

Intégration

Assurez-vous que les applications et services clés sont prêts pour la YubiKey

Lancement

Distribuez les clés aux utilisateurs via des services de livraison clé en main ou des partenaires de distribution

Adoption

Favorisez leur adoption grâce à une formation et une assistance sur les bonnes pratiques

Mesure

Établissez des rapports relatifs à l'incidence sur la sécurité et la valeur commerciale

01. Planification

Définir clairement les cas d'utilisation

L'approche progressive est la meilleure façon d'assurer un déploiement fluide. Priorisez **dans un premier temps vos utilisateurs et données critiques,** avant d'aller plus loin. Hiérarchisez les cas d'utilisation et populations d'utilisateurs en fonction des risques, du lieu de travail, de l'impact sur l'entreprise et de la facilité d'intégration technique.

Déterminer les cas d'utilisation

Il existe de nombreux cas d'utilisation dans les services financiers où le MFA résistant au phishing est essentiel. Votre priorité devrait être de traiter les cas d'utilisation et les populations d'utilisateurs en fonction du risque et de l'impact sur l'entreprise, puis d'étendre à d'autres cas d'utilisation et populations. Certaines organisations choisissent de déployer un MFA résistant au phishing auprès des groupes d'employés en priorité, en raison de préoccupations liées à la sécurité ou à des exigences réglementaires. D'autres organisations peuvent préférer le déployer auprès des clients finaux (commerciaux et/ou particuliers) utilisant les services bancaires en ligne et mobiles.

Principaux scénarios d'authentification moderne et résistante au phishing

Accès privilégié

Protégez les données sensibles et les employés ciblés bénéficiant d'un accès élevé aux systèmes ou aux données.

Postes de travail partagés

Permettez un accès sécurisé et efficace aux ordinateurs partagés dans les banques et les centres d'appels, y compris dans les zones mobiles restreintes.

Télétravail

Ajoutez une couche de protection supplémentaire pour sécuriser l'accès aux plateformes VPN, IAP, IAM et IdP.

Transactions à haut risque

Fournissez une authentification renforcée pour revérifier les utilisateurs accédant à des services à haut risque ou réalisant des transactions de grande valeur.

Chaîne d'approvisionnement logicielle

Protégez l'accès au code et mettez en œuvre une signature de code fiable.

Groupes d'utilisateurs

Employés de bureau

Les attaques sophistiquées et les escalades latérales font de chaque utilisateur un utilisateur privilégié.

Centre d'appels

Vérifiez l'identité des agents de centres d'appels pour leur fournir un accès aux systèmes clés et aux postes de travail partagés, dans des environnements mobiles restreints.

Finance dans la vente au détail

Assurez une authentification fluide entre les postes de travail pour servir les clients ou autoriser des transactions.

Tiers

Fournissez une authentification renforcée pour revérifier les utilisateurs accédant à des services à haut risque ou réalisant des transactions de grande valeur.

Clients finaux

Protégez les comptes clients contre la fraude et renforcez la fidélité et la confiance grâce à des déploiements ciblés auprès de segments clés de clientèle.

Réunir les principales parties prenantes

Bien que le nombre de ressources engagées dans le projet puisse varier en fonction de l'étendue du déploiement de la YubiKey, les principales parties prenantes dans les services suivants peuvent influencer positivement la mise en œuvre du MFA résistant au phishing dans l'ensemble de l'organisation. Pour un déploiement fluide, il est important que l'ensemble des équipes coopère :

- **Informatique**
- **Sécurité**
- **Finances**
- **Service d'assistance**
- **RH/Formation et développement**

Faire appel à des experts Yubico lorsque nécessaire

S'appuyant sur des années passées à protéger certaines des entreprises les plus soucieuses de la sécurité au monde, Yubico s'efforce d'aider les entreprises à accéder facilement aux produits et services de sécurité de manière flexible et économique pour renforcer la sécurité dans l'ensemble de l'entreprise et libérer de la productivité.

Les organisations peuvent tirer un grand bénéfice d'un modèle YubiKey as a Service. Notre équipe Professional Services offre un accompagnement technique et opérationnel de premier ordre pour soutenir la mise en œuvre et le déploiement de vos YubiKeys.

YubiKey as a Service*	Yubico Professional Services		
YubiKey as a Service	YubiEnterprise Delivery	Déploiement intégral	Planification du déploiement
Facilite l'acquisition, la mise à niveau et le support des **YubiKeys** pour les entreprises	**Livraison** des YubiKeys à l'échelle mondiale, notamment dans les emplacements reculés et aux bureaux	Planification, intégration technique et assistance au déploiement **clé en main**	Démarrez votre déploiement avec des **ateliers et des projets** pour passer en revue les cas d'utilisation et développer une stratégie personnalisée

* YubiKey as a Service est accessible aux entreprises comptant 500 utilisateurs ou plus.

02. Validation

Valider le processus auprès d'un petit groupe d'utilisateurs

Validez votre processus auprès d'un petit groupe d'utilisateurs sur un cas d'utilisation prioritaire afin d'obtenir leur confirmation et leurs retours, à l'aide des bonnes pratiques, guides, vidéos et engagements de Yubico. **Testez et tirez des leçons avant de vous lancer.**

03. Intégration

Vérifier que votre environnement est compatible avec YubiKey

Les YubiKeys peuvent fonctionner avec un grand nombre de services professionnels et personnels sans partage de secrets entre les services, ce qui permet de garantir une sécurité et une confidentialité élevées à grande échelle. Une seule clé peut être utilisée avec plus de 1 000 applications et services, sécurisant ainsi la vie numérique professionnelle et personnelle de vos utilisateurs. Pour garantir une intégration fluide des YubiKeys avec les applications et services clés que vous souhaitez sécuriser, voici quelques **questions essentielles** à considérer. Notre conseil : répondez d'abord à ces questions pour votre programme pilote, et répétez cette étape à chaque nouveau déploiement.

Qui

Qui a besoin d'un accès ?

Employés, sous-traitants, tiers, chaîne d'approvisionnement

Quoi

Quelle approche d'authentification adopter ?

MFA (mot de passe et deux facteurs robustes), sans mot de passe

Où

Dans quelles parties de votre environnement faut-il une authentification robuste ?

Éléments d'infrastructure critiques, réseau, applications, outils de développement.

Comment gérez-vous les accès ?

IAM, IdP, PAM, SSO, VPN

Comment

Quel est l'impact du lieu de travail sur le déploiement ?

Travail à distance, hybride, sur site, multi-sites

Quels types d'appareils doivent être pris en charge ?

Appareils professionnels, BYOD, ordinateurs de bureau, ordinateurs portables, smartphones

Applications compatibles YubiKey

Clés de sécurité leaders du secteur, les YubiKey fonctionnent avec des centaines de produits, services et applications. Consultez la compatibilité YubiKey → ici.

> « Avec chaque utilisateur disposant d'une YubiKey, je n'ai plus à m'inquiéter des fuites d'informations d'identification. C'est une situation vraiment idéale pour un RSSI. »
>
> **Mike Schwermin** | RSSI | Afni

Se préparer au déploiement

Après vous être assuré que votre environnement est prêt à accueillir la YubiKey, il est temps de créer un plan de déploiement des YubiKeys dans votre entreprise. Optimiser le déploiement, c'est assurer la gestion des changements organisationnels par le biais de communications, de formations et d'une assistance efficaces. Yubico propose divers services professionnels pour vous aider à accélérer ce processus :

Yubico Professional Services

Planification du déploiement
Création d'un plan de déploiement

Services d'intégration
Examen de l'architecture et des infrastructures, analyse pour l'intégration des fournisseurs

Projets de mise en œuvre
Support technique sur mesure pour intégrer les YubiKeys dans votre infrastructure

Forfaits de services
Créneaux d'assistance flexibles en fonction de vos besoins

04. Lancement

Distribuer les clés et organiser la mise en service

Nous souhaitons que le déploiement soit aussi fluide que possible pour toutes vos équipes et tous vos utilisateurs. Pour cela, nous nous engageons à simplifier vos plans de déploiement et à répondre à vos questions sur la distribution des clés aux utilisateurs et la gestion du cycle de vie des YubiKeys :

Distribution

Libre-service | Partenaire de distribution | YubiEnterprise Delivery

Gestion des clés

Adoption | Assistance | Départ

Quoi ?

Accroître la sensibilisation
Créer des supports de formation et d'assistance pour les utilisateurs

Pourquoi ?

Renforcer l'engagement
Mettez en avant les bénéfices pour l'organisation et les utilisateurs

> Nous suivons le même chemin que les organisations les plus avancées au monde. Et nous déployons tous les YubiKeys. »
>
> **Mike Schwermin** | RSSI | Afni

Recommandations et bonnes pratiques pour déployer les YubiKeys

Une fois que vos utilisateurs ont reçu leurs YubiKeys, l'étape suivante consiste à enregistrer les clés sur leurs applications et appareils. Nous vous recommandons de fournir une deuxième YubiKey (de secours) à chaque utilisateur. En cas de perte d'une YubiKey, révoquez et remplacez la clé perdue. Au départ d'un utilisateur, certaines entreprises préfèrent récupérer les YubiKeys, tandis que d'autres autorisent les utilisateurs quittant l'entreprise à les conserver et à continuer de les utiliser pour leurs comptes personnels.

Offre **flexibilité et choix** dans le format YubiKey

Deux YubiKeys par personne (exemplaire de secours)

Prévoir des **clés supplémentaires** pour les nouvelles recrues ou en cas de perte/vol

Promouvoir la **sécurité** via des politiques concernant l'usage personnel

Organiser des événements pour susciter l'enthousiasme autour de l'avenir de la sécurité de votre entreprise

Événements de mise en service

Accompagnez le lancement d'une série de communications qui présentent la YubiKey aux utilisateurs : communiquez rapidement et de manière régulière. Une communication pertinente stimule l'enthousiasme des utilisateurs face aux fonctionnalités modernes de la YubiKey.

05. Adoption

Favoriser l'adoption et stimuler l'engagement

Chez Yubico, nous pensons que la réussite ne se mesure pas au nombre de YubiKeys dont vous disposez, mais au nombre de clés que votre entreprise utilise.

Si les communications au moment de la mise en service informent les utilisateurs sur **ce que sont les YubiKeys** et **le pourquoi de leur importance**, les équipes d'assistance doivent aussi être prêtes à expliquer **comment les utiliser**, en mettant à disposition des FAQ pour répondre à toutes les questions susceptibles d'être posées durant la phase d'adoption et en cas de problème (p. ex., que faire lorsque l'on a perdu sa clé).

Durant cette phase, il est crucial de former et de sensibiliser efficacement vos utilisateurs, afin de mettre en avant les avantages directs de la YubiKey pour l'entreprise, mais aussi pour eux. La YubiKey offre une expérience utilisateur simple, qui nécessite une formation minimale et une assistance continue pour les utilisateurs.

Comment ?

Informer les utilisateurs
Présenter clairement la marche à suivre pour se lancer et pour obtenir de l'aide

06. Mesure

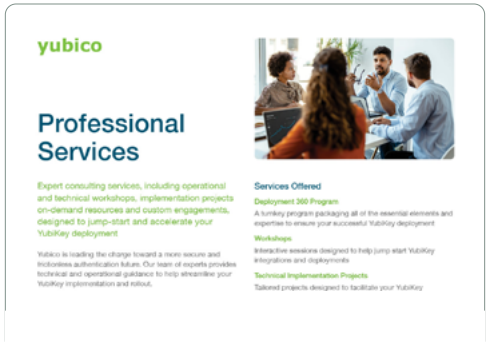
Établir des rapports relatifs à l'incidence sur la sécurité et les activités de l'entreprise

Les chiffres ne mentent pas. Évaluez la réussite de votre programme pilote sur la base des indicateurs suivants, avant d'étendre la solution à d'autres utilisateurs pour augmenter l'impact global sur l'entreprise.

Indicateurs de **déploiement** :	Indicateurs de **performance** :	Indicateurs de **sécurité** :	Indicateurs liés aux **utilisateurs** :
Nombre de clés distribuées, utilisateurs activés, applications utilisées	Réduction du temps d'assistance lié à la réinitialisation des mots de passe, augmentation de la productivité/ réduction des temps de connexion	Menaces de sécurité atténuées, simplification des contrôles de conformité ou d'audit	Facilité d'adoption, facilité d'utilisation, satisfaction

Évolutivité

Yubico propose des services de conseil spécialisés, notamment des ateliers opérationnels et techniques, des projets de mise en œuvre, des ressources à la demande et des engagements personnalisés, conçus pour lancer et accélérer votre déploiement YubiKey à grande échelle.



Téléchargez la fiche solution dédiée aux services professionnels → ici.

YubiKey as a Service*		Yubico Professional Services		
YubiKey as a Service	YubiEnterprise Delivery	Planification du lancement	Formation et assistance	Analyses et rapports
Approvisionnement et mise en œuvre économique et flexible des YubiKeys	**Livraison** des YubiKeys à l'échelle mondiale, notamment dans les emplacements reculés et aux bureaux	Création d'un plan marketing et d'un **plan de communication** adapté à vos utilisateurs	Processus et **supports de formation et d'assistance** détaillant les bonnes pratiques	**Indicateurs** et tableaux de bord personnalisés

* YubiKey as a Service est accessible aux entreprises comptant 500 utilisateurs ou plus.

> « Je suis habitué aux offres par abonnement dans le cloud, et le modèle YubiKey as a Service présente des avantages utiles qui correspondaient parfaitement à nos besoins. »
>
> **Mike Schwermin** | RSSI | Afni

YubiKey as a Service

Bénéficiez d'une sécurité basée sur l'authentification de pointe résistante au phishing pour un prix inférieur à celui d'une tasse de café par utilisateur et par mois. YubiKey as a Service, disponible par abonnement, assure votre tranquillité d'esprit dans un monde incertain.

→ **POUR EN SAVOIR PLUS, CLIQUEZ ICI**

YubiEnterprise Delivery

YubiEnterprise Delivery propose aux équipes informatiques de puissantes fonctionnalités pour gérer la livraison des clés de sécurité matérielles aux utilisateurs dans le monde entier et accélère l'adoption d'une authentification robuste.

→ **POUR EN SAVOIR PLUS, CLIQUEZ ICI**

Yubico Professional Services

Déploiement intégral

Forfaits d'heures de service

Organisation d'ateliers

Projets de mise en œuvre

Prêt à commencer ?

Il ne fait aucun doute que le MFA résistant au phishing est la solution pour sécuriser les services financiers contre les cybermenaces modernes. Bien que le chemin vers un MFA résistant au phishing et sans mot de passe puisse sembler intimidant, il ne doit pas nécessairement l'être.

Vous ne savez pas par où commencer ? La bonne nouvelle, c'est que vous n'avez pas besoin de connaître toutes les réponses à l'avance sur le nombre de clés à acheter, leur type, la manière de les intégrer à votre environnement et la façon de les mettre entre les mains des employés.

Les entreprises modernes sont conscientes que les services de sécurité sont la garantie de leur réussite. Avec YubiKey as a Service, vous avancez de manière progressive grâce à nos conseils et à notre aide. Le processus de déploiement des YubiKeys à grande échelle est simplifié et permet d'élargir le cercle des utilisateurs à mesure que les besoins de votre entreprise évoluent. Nous proposons notamment des guides et une assistance prioritaire pour vous aider à réussir votre transition le plus rapidement possible.

Besoin d'une assistance personnalisée pour l'une des six étapes de ce plan ? L'équipe Professional Services de Yubico est là pour vous aider.

Contactez-nous
yubi.co/contact

En savoir plus
yubi.co/ps

Sources

[1] IBM Cost of a Data Breach Report 2025 (Rapport sur le coût d'une brèche de données), https://www.ibm.com/reports/data-breach

[2] Shalanda D. Young, Office of Management and Budget (Gestion de bureau et budget), M-22-09 (26 janvier 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[3] Circulaire sur la sécurité nationale/NSM-8, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[4] NIST, FIPS 201-3 (janvier 2022), https://csrc.nist.gov/publications/detail/fips/201/3/final

[5] CFPB, Circulaire sur la protection financière des consommateurs 2022-04 (11 août 2022)

[6] PCI SSC, PCI DSS v4.0 (mars 2022)

yubico

À propos de Yubico

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 pour une authentification matérielle moderne, résistante au phishing, empêchant les piratages de comptes et simplifiant la connexion sécurisée.

Depuis 2007, nous avons contribué à la mise en place de standards d'authentification globaux, co-créé FIDO2, WebAuthn et FIDO U2F, et présenté la passkey originale. Aujourd'hui, notre technologie passkey sécurise des individus et des organisations dans plus de 160 pays, transformant la manière dont l'identité numérique est protégée, de l'intégration à la récupération de compte.

Plébiscitées par les plus grandes marques, les gouvernements et les institutions les plus soucieux de sécurité au monde, les YubiKeys fonctionnent immédiatement avec des centaines d'applications et de services, offrant un accès rapide, sans mot de passe, sans friction ni compromis.

Nous pensons que la sécurité renforcée ne devrait jamais être hors de portée. Grâce à notre initiative philanthropique Secure it Forward, nous faisons don de YubiKeys à des associations soutenant les communautés à risque.

Avec un double siège à Stockholm (Suède) et Santa Clara (Californie), Yubico est fier d'être reconnu parmi les 100 entreprises les plus influentes selon TIME et les plus innovantes selon Fast Company.

Pour en savoir plus, rendez-vous sur www.yubico.com.