yubico

LIVRE BLANC

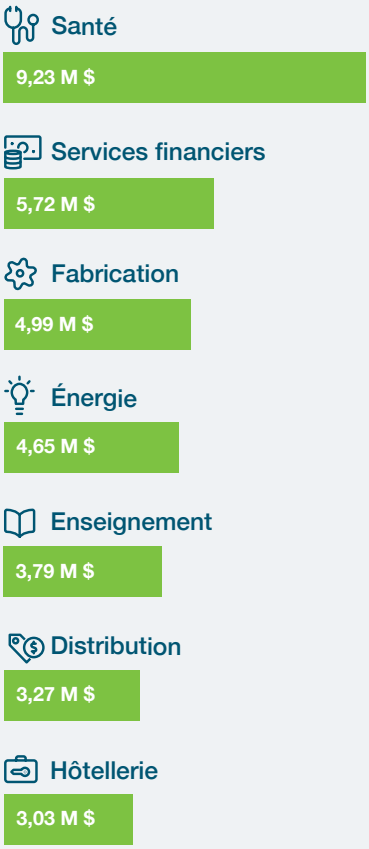
Sécuriser les postes de travail partagés contre les cybermenaces modernes

MFA résistant au phishing avec expérience utilisateur exceptionnelle

Contenu

Les postes de travail partagés sont des cibles faciles pour les cyberattaques

Coût des brèches de données par secteur[1]



Aujourd'hui, les organisations font face à l'évolution constante du paysage des cybermenaces. Cette évolution convoque l'intelligence artificielle et l'apprentissage automatique, ainsi que tout un panel de vecteurs de menaces tels que le phishing, le SIM swapping et les attaques de type Man-in-the-Middle (MiTM), qui ne cessent de gagner en sophistication. Nombre de ces approches sont pratiquement impossibles à distinguer pour l'utilisateur final. Ce dernier et son organisation sont donc extrêmement vulnérables. Les informations d'identification compromises restent le point d'entrée le plus courant des attaques : 61 % des brèches de données sont liées d'une manière ou d'une autre aux informations d'identification.[2] Les pratiques non sécurisées relatives aux informations d'identification, notamment le partage autorisé ou non des noms d'utilisateur et des mots de passe, ne font qu'aggraver les risques de brèches de données pour les organisations.

Les postes de travail partagés sont courants dans les secteurs de la santé, de la fabrication, de la distribution, de l'hôtellerie, des services financiers, de l'énergie, des services publics, du pétrole et du gaz, et de l'éducation. Ces environnements sont caractérisés par des roulements d'équipes importants, des employés saisonniers et un taux de rotation élevé. Dans ces conditions, les risques potentiels pour la sécurité sont élevés si des mesures de protection rigoureuses ne sont pas mises en place. Les postes de travail partagés amplifient la menace interne, qu'il s'agisse de malveillance ou de négligence, et présentent des risques de sécurité supplémentaires lorsqu'ils sont utilisés dans des zones très fréquentées. Les pratiques non sécurisées, telles que le partage de mots de passe et leur inscription sur des notes autocollantes, sont courantes dans les environnements où les postes de travail et les appareils sont partagés et utilisés par les employés travaillant par roulement. Elles témoignent de problèmes systémiques liés aux processus d'authen-tification qui entravent la réalisation de certaines tâches essentielles.

61 %

des brèches de données sont liées aux **informations d'identification**[3]

11,45 Mio. USD

le coût moyen total des menaces internes[4]

46 %

des employés **partagent des mots de passe** ou des comptes[5]

82 %

des personnes **réutilisent leurs mots de passe** sur plusieurs comptes[6]

41 %

utilisent des notes autocollantes pour la gestion des mots de passe[7]

Qu‘est-ce qu‘un poste de travail partagé ?

Les postes de travail partagés sont des appareils utilisés par plusieurs personnes, parfois appelés « utilisateurs itinérants ». Plusieurs employés s‘authentifient sur le même poste de travail tout au long de la journée, comme dans les centres d‘appels ou sur les terminaux de point de vente. Les postes de travail partagés sont monnaie courante dans les secteurs où le personnel travaille par roulement, en alternant les postes tout au long de la journée, ou dans les secteurs qui emploient des travailleurs à l‘heure, des travailleurs intérimaires ou saisonniers.

Les postes de travail, les terminaux et les appareils partagés sont essentiels au fonctionnement quotidien des entreprises d‘un large éventail de secteurs d‘activité. Ces dispositifs sont souvent en lien direct avec des systèmes et des données critiques, notamment les données clients, les informations de paiement, les informations propriétaires, les chaînes de fabrication ou d‘assemblage, voire les informations de santé protégées.

De par leur nature même, les postes de travail partagés constituent des cibles faciles pour les cybercriminels et les attaques internes :

- **Ont plusieurs utilisateurs**
- **Utilisés dans les zones très fréquentées**
- **Accès aux systèmes ou données critiques**
- **Généralement sujets à des pratiques de sécurité peu sûres**
- **Peuvent ou non être gérés par l‘entité juridique**

Les postes de travail partagés amplifient les risques liés aux périphériques, à l‘accès des utilisateurs, à l‘authentification ou aux menaces internes qui entraînent le vol ou la perte d‘informations d‘identification, de données stratégiques ou de propriété intellectuelle. Si un poste de travail partagé est indisponible suite à une cyberattaque, cela peut entraîner une interruption de l‘activité et d‘autres répercussions touchant au chiffre d‘affaires, à la réputation de la marque et aux sanctions pour non-respect de la réglementation.

Scénarios courants de postes de travail partagés et vulnérabilités associées

Secteurs où les terminaux sont partagés

- Accueil dans la distribution et l'hôtellerie
- Poste de soins en hôpital ou clinique
- Station de fabrication ou logistique

Secteurs mobiles restreints

- Centres d'appels
- Salles blanches
- Environnements physiquement isolés
- Sites de haute sécurité
- Sites industriels (pas de connexion, plates-formes pétrolières, etc.)

Terminaux partagés

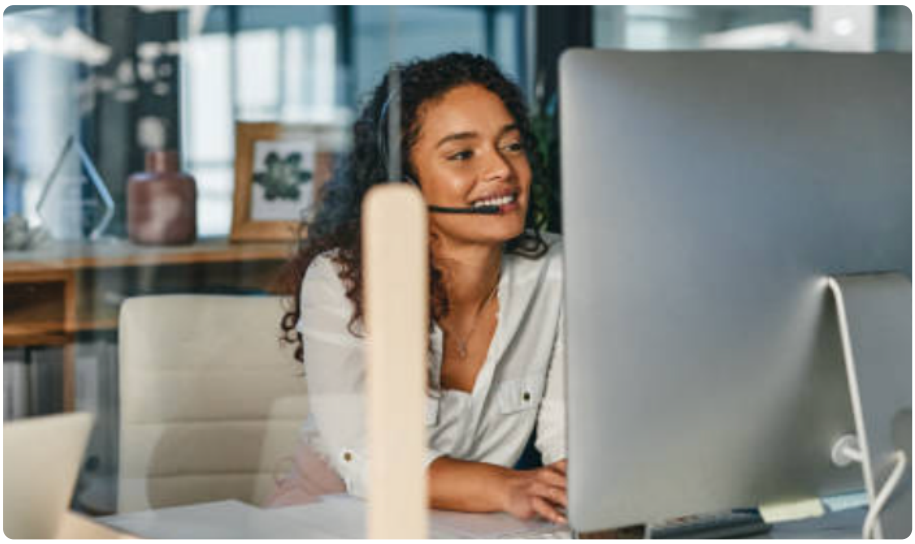
Les terminaux partagés sont des postes de travail offrant un ensemble d'applications courantes partagées par un grand nombre d'utilisateurs différents dans des environnements d'accueil (restaurant, hôtel, banque, bureau de poste, commerce de détail), dans les postes de soins ou dans des environnements de fabrication et de logistique. Les terminaux partagés peuvent être fixes ou portatifs, comme c'est le cas pour les postes de travail mobiles dans le secteur de la santé.

Les terminaux partagés sont souvent utilisés par plusieurs utilisateurs en même temps. Ceci accroît la prévalence des pratiques peu sûres liées au partage des mots de passe afin de réduire le temps de déconnexion et de connexion nécessaire pour accéder aux ressources partagées. Dans le secteur de la santé, par exemple, le partage de mots de passe entre les professionnels de santé reste répandu (73,6 %), tandis que les niveaux d'accès individuels sont les mêmes.[8]

Environnements mobiles restreints

Un environnement mobile restreint est un environnement dans lequel les appareils mobiles ne peuvent pas être utilisés. Cela peut être dû à des facteurs liés à l'environnement lui-même, tels que des réseaux physiquement isolés, des environnements difficiles, des sites hors ligne ou offshore, des salles blanches ou des sites de haute sécurité. Cette situation tient parfois à des restrictions imposées par des réglementations ou des syndicats, ou encore à la politique de l'entreprise qui décourage l'utilisation d'appareils mobiles. Un sous-ensemble d'employés au sein d'une organisation peut également ne pas souhaiter utiliser d'appareils mobiles personnels à des fins professionnelles, ce qui nécessite une méthode d'authentification différente.

Les postes de travail et périphériques partagés dans les environnements mobiles restreints exigent une authentification hautement sécurisée, conforme aux réglementations sectorielles et simple à utiliser, afin de favoriser l'adoption par les utilisateurs.



Secteurs « grab-and-go »

- Agents de police et de sécurité
- Santé et soins à domicile
- Visite à des tiers

Environnement « grab-and-go »

Un environnement « grab-and-go » prévoit généralement l'utilisation d'un ensemble mobile d'appareils partagés qui peuvent être récupérés et utilisés dans les locaux d'une entreprise ou sur des sites distants. Il peut s'agir d'un appareil informatique moderne tel qu'un ordinateur portable, une tablette ou un téléphone mobile, ou même d'un appareil lié à un système classique. Les appareils partagés de type « grab-and-go » sont courants dans les établissements d'enseignement, les bibliothèques, les forces de l'ordre et les services de santé. Dans chacun de ces environnements, l'utilisateur n'a besoin de l'appareil que pour une période limitée.

En outre, de nombreux secteurs ont répondu aux réalités du travail hybride post-pandémique en offrant davantage de possibilités de travail nomade aux employés susceptibles de privilégier des configurations fixes à domicile. Au lendemain de la pandémie, les employés considèrent les appareils « grab-and-go » et la réservation d'un espace de travail en entreprise comme une option de travail flexible et attrayante.[9]

Comme aucun utilisateur n'est associé à l'appareil, il est important de mettre en place des contrôles qui n'accordent l'accès qu'aux applications et services associés aux informations d'identification d'un utilisateur particulier, et d'assurer une authentification rapide et fiable afin de favoriser la productivité.

Secteurs avec points de vente

- Distribution
- Épicerie
- Vente en gros

Terminal point de vente (TPV)

Ces postes de travail spécialisés, dédiés aux transactions financières en contact direct avec les clients dans les commerces de détail et d'alimentation, les restaurants et les fast-foods, ou encore les environnements de vente en gros, peuvent être utilisés par les employés ou même par les clients (terminaux en libre-service). Afin d'optimiser l'expérience client, une attention particulière doit être accordée à la rapidité et à la facilité d'authentification, en évitant le verrouillage potentiel des comptes et, surtout, en garantissant la sécurité des informations relatives aux clients et aux paiements.

En raison du risque élevé pour les données financières sur les TPV, ces postes de travail sont fortement réglementés par la norme PCI DSS (Payment Card Industry Data Security Standard). Le skimming de carte est le risque le plus courant avec les terminaux de point de vente, saisissant les données provenant de l'infrastructure de paiement, par superposition, avec des malwares ou compromis, ou en interceptant les données sans fil/NFC. Le taux élevé de rotation des employés et la nature du travail saisonnier créent souvent des points de pression supplémentaires concernant l'intégration et la désactivation de l'accès des employés aux systèmes TPV.

L'utilisation de smartphones, de tablettes ou d'autres périphériques sans fil au lieu d'un TPV standard est un sujet de préoccupation croissant dans les points de vente. D'ici 2023, on estime que 1 transaction en point de vente sur 4 se fera via mPOS (mobile point-of-sale), un processus qui augmente le risque d'attaques de type Man-in-The-Middle (attaque MiTM) et introduit d'autres vulnérabilités mobiles.[10]

> L'authentification multi-facteurs (MFA) est essentielle, mais toutes les méthodes MFA ne se valent pas. Twitter utilisait une solution MFA basée sur application, qui envoyait une demande d'authentification sur le smartphone de l'employé. Il s'agit d'une forme courante de MFA, mais elle peut être contournée. Lors du piratage de Twitter, les pirates ont contourné la solution MFA en convainquant les employés de la société de confirmer le MFA basé sur l'application lors de la connexion. Une clé de sécurité physique, ou MFA matériel, est la forme la plus sûre d'authentification multi-facteurs (MFA). Il s'agit d'une clé USB qui est connectée à un ordinateur et sert à l'authentification de l'utilisateur. Ce type de MFA matériel, qui aurait permis d'arrêter les pirates, est désormais mis en œuvre par Twitter à la place du MFA basée sur l'application."
>
> New York Department of Financial Services, Twitter Investigation Report, oktobre 2020

Quatre exigences d'authentification critiques sur les postes de travail partagés

Sécurité | Efficacité | Fiabilité | Coût

Lorsqu'elles envisagent des solutions d'authentification pour les environnements à postes de travail partagés, les organisations doivent dans un premier temps tenir compte de l'efficacité de la solution en matière de protection contre les cyberattaques externes et les menaces internes. Elles doivent, en outre, s'interroger sur l'impact de la solution sur la productivité des utilisateurs (verrouillage des comptes, temps de connexion), sur la fiabilité de la solution dans divers environnements et cas d'utilisation, sur les variables externes susceptibles d'avoir un impact négatif sur les performances, telles que le signal cellulaire et les batteries, ainsi que sur le coût total de possession à long terme.

Voici les quatre exigences d'authentification critiques que les entreprises doivent prendre en compte pour tout environnement à postes de travail partagé :

Sécurité

Comment s'assurer que l'utilisateur qui se connecte à l'appareil est la personne légitime ?

Comment sécuriser les appareils partagés et les ressources internes avec plusieurs utilisateurs en rotation, en s'assurant que les comptes utilisateurs sont sûrs et que les utilisateurs n'ont accès qu'aux applications, services et données auxquels ils doivent avoir accès ?

Les comptes administrateurs ou les postes de travail partagés avec accès à des informations privilégiées doivent être protégés par un mécanisme d'authentification qui rend impossible l'usurpation d'identité.

Les postes de travail partagés doivent s'appuyer fortement sur les autorisations des utilisateurs et les contrôles d'accès (pas de connexions partagées, d'invités ou anonymes), et présenter des restrictions empêchant la sauvegarde des mots de passe. Les comptes administrateurs doivent également être individuels et non partagés, afin de permettre un dépannage en personne ou à distance.

Il faut tenir compte du temps nécessaire à l'authentification et du nombre de fois qu'un utilisateur doit s'authentifier au cours d'une journée ou d'un quart de travail.

Efficacité

Comment s'assurer que l'utilisateur peut s'authentifier rapidement et simplement ?

Tout mécanisme d'authentification adopté pour les postes de travail partagés doit permettre aux employés de s'authentifier rapidement et facilement, afin d'éviter les perturbations du flux de travail et les solutions de contournement non approuvées. Actuellement, 54 % des employés pensent que les solutions d'authentification à deux facteurs telles que l'OTP et les codes push perturbent leur flux de travail quotidien.[11] De plus, 34 % des employés ont été confrontés à une impossibilité d'accéder à des informations professionnelles critiques parce qu'ils n'avaient pas accès à un téléphone ou à une application d'authentification.[12]

Comme mentionné précédemment, toutes les formes d'authentification multi-facteurs (MFA) n'offrent pas l'équilibre optimal entre une sécurité renforcée et une expérience utilisateur simple et rapide qui favorise une productivité élevée. Certains authentificateurs mobiles peuvent accroître le nombre d'étapes du processus d'authentification. Les utilisateurs doivent attendre des codes OTP ou push dans une application, ou dans le cas d'organisations pharmaceutiques, de soins de santé et de produits chimiques, retirer l'équipement de protection individuelle (EPI) pour s'authentifier. Quel que soit le scénario, il faut tenir compte du temps nécessaire à l'authentification et du nombre de fois qu'un utilisateur devra s'authentifier au cours d'une journée ou d'un quart de travail. Lorsque les exigences d'efficacité sont élevées, une expérience d'authentification sans mot de passe peut être envisagée.

Fiabilité

Comment garantir une authentification fiable, qui fonctionne même dans des environnements difficiles avec différents degrés de connexion ?

L'authentification est un service stratégique. Si les employés ne peuvent pas se connecter aux applications ou aux portails qu'ils utilisent, ils ne peuvent pas faire leur travail. Toute solution d'authentification doit être fiable pour chaque utilisateur et exclure les points de défaillance courants, qu'il s'agisse de la connectivité, de la batterie de l'appareil, de la réception cellulaire ou de jetons matériels. Les solutions d'authentification doivent également être dotées de fonctionnalités telles que la technologie NFC, adaptées à des environnements tels que les laboratoires, la fabrication industrielle, les salles blanches et d'autres types d'environnements caractérisés par une atmosphère explosive.

Il faut savoir que toute solution d'authentification reposant sur « quelque chose que vous connaissez » (comme un mot de passe) est sujette à l'erreur humaine (perte, oubli ou erreur de frappe) qui alourdit l'expérience d'authentification et risque de bloquer l'accès des utilisateurs à leurs comptes. Les solutions d'authentification mobiles ne sont pas toujours fiables dans les environnements à postes de travail partagés, où la couverture cellulaire est irrégulière ou inexistante. C'est le cas par exemple sur les plateformes offshore, dans les environnements de technologie opérationnelle (OT) et dans les zones géographiques reculées, ou lorsque les utilisateurs dépendent de la batterie de l'appareil dans le cas de l'authentification mobile.

> “En moyenne, une entreprise perd 5,2 millions de dollars en termes de productivité par an en raison de verrouillages de compte.”
>
> Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report

Coût

Comment réduire le nombre de tickets d‘assistance liés à l‘authentification ?

Toute forme d‘authentification classique, comme les noms d‘utilisateur et les mots de passe, et l‘authentification mobile appliquée et mise en œuvre à grande échelle, nécessitera une mise en œuvre des politiques, une formation des utilisateurs et une assistance informatique permanentes. Toutes les formes d‘authentification mobile, telles que les SMS, les OTP et les notifications push, peuvent représenter une charge de travail considérable pour l‘assistance si les codes tardent à arriver, si les utilisateurs se voient bloquer l‘accès à leur compte ou s‘ils doivent enregistrer de nouveaux appareils.

Chaque fois qu‘un utilisateur rencontre des difficultés avec l‘authentification mobile, il n‘est pas productif. Plus vite un utilisateur peut s‘authentifier et faire son travail en toute sécurité, ou même réinitialiser son mot de passe par lui-même si nécessaire, meilleur est le retour sur investissement.

Inconvénients de l‘authentification multi-facteurs (MFA) classique

Sécurité et fiabilité faibles, coût et frustration élevés

Les informations d‘identification restent l‘une des principales cibles des cyberattaquants et sont associées à 61 % des violations de données.[13] L‘employé moyen doit utiliser et retenir 191 mots de passe, facteur de complexité et de frustration pour les utilisateurs.[14] À l‘heure actuelle, pour une entreprise moyenne, 60 % des interactions avec le service d‘assistance informatique sont liées à la réinitialisation des mots de passe.[15] Outre les coûts informatiques, les entreprises perdent en moyenne 5,2 millions de dollars par an en termes de productivité suite au verrouillage des comptes.[16]

Vers quoi la frustration permanente relative à l‘authentification tend-elle le plus souvent ? Des solutions de contournement risquées, même pour les utilisateurs les plus avertis. En fait, 49 % des professionnels de la sécurité informatique admettent partager des mots de passe.[17] Nous savons que les postes de travail partagés présentent des taux plus élevés de partage de mots de passe, de réutilisation de mots de passe entre comptes, ou d‘enregistrement de mots de passe dans le navigateur ou l‘application. Ces pratiques ne sont jamais sûres, elles amplifient le risque dans un scénario de poste de travail partagé.

Cependant, il convient de noter que si toute forme d‘authentification à deux facteurs résistante au phishing (2FA) ou d‘authentification multi-facteurs (MFA) offre plus de sécurité que les mots de passe seuls, les mots de passe restent leur premier facteur. En outre, dans le cas de l‘authentification multi-facteurs (MFA) classique, comme l‘authentification multi-facteurs (MFA) mobile, le second facteur est lié à l‘appareil mobile. Il s‘agit d‘un signal d‘alarme pour trois raisons : il n‘y a aucune garantie réelle que la clé privée se retrouve sur un élément sécurisé de l‘appareil mobile, le code OTP ou la clé privée risquent d‘être interceptés, et il est impossible d‘assurer la preuve de la possession ; ou, selon les termes du National Institute of Standards and Technology (NIST), impossible de prouver la résistance à l‘usurpation d‘identité.

Les clés de sécurité matérielles FIDO2 offrent une authentification multi-facteurs et sans mot de passe, avec une sécurité élevée et une expérience utilisateur exceptionnelle. Elles constituent également une chaîne de confiance portative qui convient parfaitement aux environnements à postes de travail partagés.

L'authentification mobile classique est sujette aux cyberattaques modernes, notamment le phishing, les attaques par force brute, les attaques de type Man-in-The-Middle (attaque MiTM), les malwares et le SIM swapping. Outre les questions de sécurité, l'authentification mobile classique comporte de nombreux coûts cachés liés à la perte de productivité, au coût des appareils, à une assistance informatique accrue et à des frictions au niveau de l'expérience utilisateur. En fait, 43 % des organisations citent l'expérience utilisateur comme le principal obstacle à l'utilisation d'une solution MFA.[19] Pour en savoir plus, consultez notre livre blanc :r: Les 5 principales idées reçues concernant l'authentification mobile : déconstruire le mythe par rapport à la réalité du MFA classique.

Le remplacement de l'authentification à facteur unique (nom d'utilisateur et mot de passe) classique par un MFA résistant au phishing est la première étape du renforcement des pratiques de sécurité.

Les actions de l'utilisateur étant en fin de compte la plus grande faiblesse de l'authentification classique, et l'authentification en plusieurs étapes contribuant fortement à l'insatisfaction de l'utilisateur, la meilleure pratique mondiale tend vers une authentification sans mot de passe, c'est-à-dire une authentification qui n'exige pas de l'utilisateur qu'il fournisse un mot de passe lors de la connexion.

Le passage de l'authentification multi-facteurs (MFA) classique au MFA résistant au phishing est une étape clé dans la sécurisation des environnements à postes de travail partagés. La prochaine étape de l'authentification multi-facteurs (MFA) moderne consiste à introduire l'authentification sans mot de passe. L'utilisation des mots de passe à usage unique par SMS (OTP) est une forme d'authentification sans mot de passe, jugée faible du point de vue de la sécurité. Les cartes à puce traditionnelles sont une autre forme d'authentification sans mot de passe qui offre une sécurité élevée, mais elles nécessitent généralement des investissements considérables en lecteurs de cartes à puce, cartes et plates-formes de gestion back-end. De plus, elles n'offrent pas zet les tablettes. C'est pourquoi l'industrie s'oriente vers un flux de connexion moderne sans mot de passe en s'appuyant sur FIDO2/WebAuthn.

FIDO (Fast Identity Online) est une norme d'authentification moderne qui remplace le nom d'utilisateur et le mot de passe traditionnels par une authentification forte à deux facteurs, multi-facteurs et sans mot de passe. La norme FIDO a été créée par la FIDO Alliance, une association industrielle ouverte dont la mission est de réduire la dépendance aux mots de passe. FIDO2/WebAuthn est la norme FIDO la plus récente. Elle fait appel à la cryptographie à clé publique pour une sécurité élevée, les clés privées ne quittant jamais l'authentificateur. Les clés de sécurité matérielles FIDO2 offrent une authentification multi-facteurs et sans mot de passe, avec une sécurité élevée et une expérience utilisateur exceptionnelle. Elles constituent également une chaîne de confiance portative qui convient parfaitement aux environnements à postes de travail partagés.

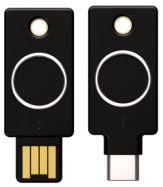
Sécurisation des postes de travail partagés avec un MFA résistant au phishing

La YubiKey offre une défense solide contre le phishing, une portabilité et une expérience utilisateur exceptionnelle

Google: quelle est l'efficacité d'une hygiène de base sur un compte dans la prévention du piratage ? (article en anglais)

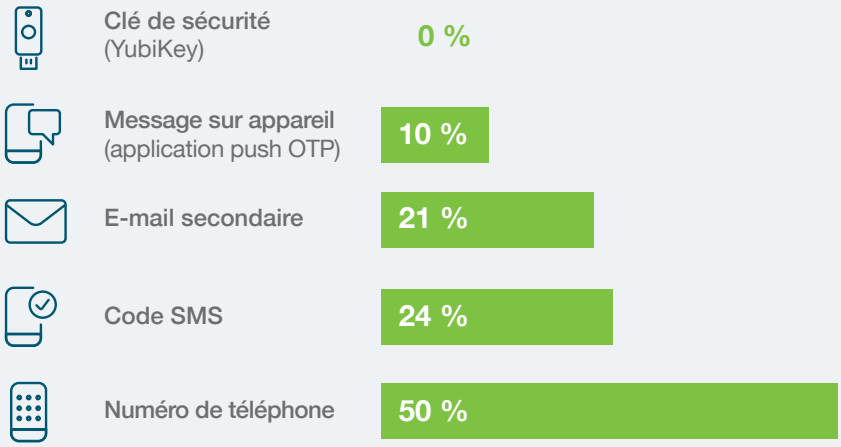
La série YubiKey 5
De gauche à droite : YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano et YubiKey 5C Nano

La série YubiKey 5 CSPN
De gauche à droite : YubiKey 5 NFC CSPN, YubiKey 5C NFC CSPN, YubiKey 5Ci CSPN, YubiKey 5C CSPN, YubiKey 5 Nano CSPN et YubiKey 5C Nano CSPN



YubiKey Bio Series – Édition FIDO
De gauche à droite : YubiKey Bio - Édition FIDO, YubiKey C Bio - Édition FIDO

Taux de prévention des piratages de comptes[18]



Yubico a créé la YubiKey, une clé de sécurité matérielle résistante au phishing offrant une expérience utilisateur exceptionnelle dans un format portatif USB et nano. Avec la YubiKey, les utilisateurs peuvent s'authentifier facilement et en toute sécurité sur plus de 700 applications et services sur une variété d'appareils, d'un simple contact ou d'une simple pression.

La YubiKey propose une authentification à deux facteurs, multi-facteurs et sans mot de passe, résistante au phishing, à grande échelle, l'authentificateur matériel protégeant les secrets et tout ce qui est confidentiel sur un élément sécurisé difficilement exfiltrable. La YubiKey est la seule solution pour laquelle des études indépendantes ont prouvé qu'elle empêchait 100 % des piratages de comptes.[20]

La YubiKey emploie des protocoles d'authentification modernes tels que les normes d'authentification ouvertes FIDO U2F et FIDO2 pour éliminer les attaques par phishing visant les informations d'identification. Les YubiKeys prennent également en charge les protocoles SmartCard, OTP et OpenPGP, ce qui permet l'utilisation d'une clé de sécurité unique sur une grande variété de systèmes modernes et classiques. Polyvalente, la YubiKey ne nécessite pas d'installation logicielle, de batterie ou de connexion cellulaire. Il s'agit de la solution idéale pour les postes de travail partagés et les environnements mobiles restreints, y compris les zones isolées. Les utilisateurs profitent d'un flux de travail d'authentification harmonieux : il suffit d'insérer la YubiKey dans un port USB et d'appuyer sur un bouton pour s'authentifier, ou de rapprocher la YubiKey d'un appareil utilisant la technologie NFC (parfaitement adapté aux zones à risque d'explosion).

Les YubiKeys constituent en outre une passerelle vers l'authentification sans mot de passe avec prise en charge de plusieurs protocoles d'authentification. Afin de renforcer l'expérience utilisateur et la rapidité d'authentification, Yubico propose également la YubiKey Bio Series-Édition FIDO. Cette clé prend en charge FIDO U2F et FIDO2, et assure la sécurité caractéristique de toutes les YubiKeys, avec une nouvelle expérience sans mot de passe basée sur la biométrie.

Cas d‘utilisation du secteur

> “Plutôt que de recommander YubiKey à nos clients, nous nous efforçons d’en faire une solution obligatoire. Nous l’intégrons dans notre suite d’hébergement et dans nos frais d’utilisation.”
>
> **Retail Control Systems**

Protection des renseignements personnels et financiers confidentiels dans les centres d‘appel des banques de détail

En 2019, Aite Group a interrogé 25 cadres de 18 des 40 plus grandes institutions financières américaines. Il en ressort que 61 % des fraudes ont pour origine le centre de contact.[21] Avec un taux de rotation élevé des employés, des pics saisonniers et d‘autres dynamiques commerciales difficiles, les environnements à postes de travail partagés des centres d‘appels exigent une approche simple et sécurisée pour vérifier l‘identité des agents avant de leur donner accès à des systèmes critiques et à des informations personnelles identifiables.

En déployant des YubiKeys, les centres d‘appels des services financiers se dotent d‘une sécurité renforcée. Ainsi, l‘identité des agents du centre peut être vérifiée en toute sécurité avant qu‘ils n‘aient accès aux informations personnelles identifiables et autres données sensibles, ou qu‘ils n‘effectuent des changements sur le compte d‘un client, comme l‘augmentation d‘une limite de crédit. En pratique, la YubiKey a permis de réduire le coût total de possession dans les environnements de centre d‘appels, éliminant ainsi la nécessité d‘actualiser fréquemment les mots de passe, les verrouillages de compte et les coûts d‘assistance informatique, tout en rationalisant la productivité des employés. Pour plus de détails, consultez le livre blanc : Les fondamentaux d’une authentification forte dans les centres d‘appels des services financiers.

Sécuriser les postes de travail du personnel infirmier et les appareils « Tap-and-Go » dans les hôpitaux

Les établissements de santé restent la cible privilégiée pour le vol de données. La sécurisation de l‘accès aux postes de travail partagés et aux périphériques « Tap-and-Go » utilisés pour les tournées constitue donc un défi.

La plupart des hôpitaux disposent de systèmes de badges pour accéder aux postes de travail et appareils partagés. Or, dans le cas d‘un accès élevé (pour l‘accès administrateur ou pour la prescription électronique de substances contrôlées, ou EPCS), ces systèmes font toujours appel à l‘authentification à deux facteurs avec des mots de passe, l‘authentification mobile ou des données biométriques. Ainsi, et contrairement aux cartes à puce, les YubiKeys dotées de la technologie sans mot de passe FIDO2 peuvent fournir une authentification renforcée par cowntact ou pression et un code PIN stocké et vérifié localement sur la clé sans recourir à des pilotes matériels supplémentaires.

Pour plus d‘informations sur l‘utilisation du MFA résistant au phishing par YubiKey dans le secteur de la santé, consultez le livre blanc : Les fondamentaux d‘une authentification forte dans les centres d‘appels des services financiers.

Des TPV sécurisés, pratiques et fiables

Retail Control Systems (RCS) commercialise et prend en charge la gestion commerciale et les systèmes de point de vente (TPV) pour les commerçants et les restaurants. Soumis à des exigences de conformité PCI (Payment Card Industry) de plus en plus strictes, RCS recherchait une solution qui pourrait être utilisée en interne pour sécuriser l‘accès administrateur à distance aux systèmes, mais aussi en externe pour protéger l‘accès aux données sensibles.

Aujourd‘hui, RCS authentifie plus de 11 000 connexions d‘utilisateurs avec des YubiKeys dans une période type de 48 heures, protégeant ainsi les périphériques ainsi que des utilisateurs particuliers et des profils d‘utilisateurs partagés.

Résumé

La YubiKey est une solution extrêmement résistante et fiable (certifiée IP68), qui offre une sécurité élevée et une expérience utilisateur exceptionnelle. Elle remplace les facteurs secondaires chronophages et non sécurisés par une expérience utilisateur « Tap-and-Go » fiable, et réduit également les coûts d'assistance informatique.

Afin de garantir une sécurité renforcée pour vos environnements à postes de travail partagés, la YubiKey est spécialement conçue pour répondre aux besoins des organisations et des utilisateurs, offrant une grande résistance au phishing. Elle offre des fonctionnalités MFA modernes et vous aide même à faire la transition vers l'abandon total des mots de passe, pour une meilleure expérience utilisateur et une efficacité globale accrue. Gardez une longueur d'avance sur les menaces en constante évolution. Grâce à une sécurité de premier ordre, vous définissez les conditions de votre réussite, non seulement aujourd'hui, mais aussi pour demain.

La YubiKey offre un MFA moderne et résistant au phishing, et favorise la transition vers l'auth-entification sans mot de passe pour une meilleure expérience utilisateur et une efficacité globale accrue.

	Nom d'utilisateur et mot de passe	Authentificateurs mobiles	YubiKey
Sécurité	Faible, facilement piratée	Taux moyens de piratage de compte de 10 à 15 %[22]	Élevée,0 % de piratage de compte[23]
Efficacité	Frustration liée aux mots de passe, verrouillages de compte	Utilisateurs qui ne peuvent/veulent pas utiliser le MFA mobile	Expérience tactile Connexion 4x fois plus rapide que l'OTP[24]
Fiabilité	Sujette à l'erreur humaine	Tributaires de la batterie de l'appareil et du réseau cellulaire. Ne conviennent pas aux environnements mobiles restreints	Construction robuste, indépendante du réseau cellulaire
Coût	Aucun coût initial Dépenses IT élevées Risque élevé	1 840 $: le coût réel de la mobilité d'entreprise par périphériquedétenu[25]	Faible coût par rapport à l'authentification multi-facteurs (MFA) mobile et réduction de 92 % des tickets d'assistance[26]

Sources

[1] BM, 2021 Cost of Data Breach Report, (consulté le 14 septembre 2021),

[2] IBM, 2021 Cost of Data Breach Report, (consulté le 14 septembre 2021); Verizon, 2021 Data Breach investigations Report, (consulté le 18 mai 2021)

[3] IVerizon, 2021 Data Breach investigations Report, (consulté le 18 mai 2021)

[4] IBM, Cost of Insider Threats: Global Report 2020, (consulté le 12 novembre 2021)

[5] Keeper, 4 Rules for Safe Password Sharing in the Workplace (avril 2021)

[6] IBM, 2021 Cost of Data Breach Report, (consulté le 14 septembre 2021)

[7] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (février 2020)

[8] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (février 2020); Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (juillet 2017)

[9] Simon Constable, How Hot Desking Will Kill Your Company (20 juin 2019); Jessica Dickler, Post-pandemic, the office will now have a whole new look, (12 juillet 2021)

[10] Juniper Research, POS & mPOS Terminals: Market Summary & Key Takeaways, (consulté le 10 novembre 2021); Charlie Osborne, PayPal, Square vulnerabilities impact mobile point-of-sale machines (10 août 2018)

[11] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (février 2020); Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (juillet 2017)

[12] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (février 2020); Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (juillet 2017)

[13] Verizon, 2021 Data Breach investigations Report, (consulté le 18 mai 2021)

[14] Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé, (1er novembre 2017)

[15] Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests, (août 2019)

[16] Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (consulté le 14 septembre 2021)

[17] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (février 2020); Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (juillet 2017)

[18] 451 Research, 2021 Yubico and 451 Research Study, (avril 2021)

[19] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (17 mai 2019)

[20] Aite Group for PinDrop, 61% of Fraud Traced Back to the Contact Center, (consulté le 15 novembre 2021)

[21] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[22] Ibid.

[23] Ibid.

[24] Wander: Uncovering the true costs of enterprise mobility

[25] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

yubico

À propos de Yubico

Yubico (Nasdaq First North Growth Market Stockholm : YUBICO), l'inventeur de la YubiKey, fait figure de référence en matière d'authentification multi-facteurs (MFA) résistante au phishing, prévenant les piratages de compte et simplifiant la sécurisation des connexions pour tous. Depuis sa création en 2007, il a joué un rôle de premier plan dans la mise en œuvre de standards mondiaux pour l'accès sécurisé aux ordinateurs, aux appareils mobiles, serveurs, navigateurs et comptes sur Internet. Yubico est l'un des créateurs et principaux contributeurs des standards d'authentification ouverts FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F), et un pionnier de l'authentification par passkeys matérielles moderne et sécurisée à grande échelle, avec des clients dans plus de 160 pays.

Les solutions de Yubico permettent des connexions sans mot de passe utilisant la forme la plus sécurisée de la technologie passkey. Les YubiKeys sont prêtes à l'emploi dans des centaines d'applications et de services destinés aux particuliers et aux entreprises, faciles et rapides à utiliser, et offrent une sécurité rigoureuse.

Fidèle à sa mission de sécuriser Internet pour tous, Yubico fait don de YubiKeys à des organisations qui aident les personnes à risque par le biais de l'initiative philanthropique Secure it Forward. Ses sièges sociaux sont situés à Stockholm et à Santa Clara, en Californie. Pour plus d'informations sur Yubico, rendez-vous sur www.yubico.com.