

## Le spécialiste des centres de contact Afni réduit ses primes d'assurance contre les cyberattaques de 30 % grâce aux YubiKeys

Protection contre les cyberattaques ciblées grâce à l'authentification multi-facteurs (MFA) résistant au phishing

### Étude de cas



#### Secteur

- Externalisation des processus métier

#### Avantages

- Réduction de 30 % des taux d'assurance contre les cyberattaques
- Intégration transparente à Microsoft Azure AD
- Authentification multi-facteurs (MFA) résistant au phishing pour l'accès aux données des clients

#### Protocoles

- WebAuthn/FIDO2

#### Produits

- YubiKey 5C NFC

#### Informations sur le déploiement

- Couverture MFA à 100 %
- Déploiement échelonné pour l'ensemble des 10 000 employés
- Centres d'appel mondiaux, employés de bureau et travailleurs à distance

## Le spécialiste de l'engagement client Afni renforce son programme de cybersécurité grâce à l'authentification multi-facteurs (MFA) résistant au phishing

Basée à Bloomington, dans l'Illinois (États-Unis), Afni est dans le secteur de l'engagement client depuis 1936, s'appuyant sur son expérience dans les recouvrements et la subrogation d'assurance pour offrir des services complets sur les canaux entrants, sortants et numériques à travers le monde. Les offres de services d'Afni couvrent l'intégralité du cycle de vie d'une relation client, de la vente et la croissance à l'assistance et à la fidélisation client. Comme toute entreprise d'externalisation des processus métier, Afni est de plus en plus la cible d'attaques sophistiquées en raison de son rôle de partenaire de confiance dans la chaîne d'approvisionnement d'autres organisations, avec un accès aux données clients, notamment dans les systèmes de télécommunications, d'assurance et de santé. Par conséquent, Afni réévalue constamment ses programmes de cybersécurité pour maintenir la confiance de ses clients.

Il y a un peu plus d'un an, Afni a nommé Brent Deterding comme nouveau responsable de la sécurité des systèmes d'information (RSSI), car il apporte près de 20 ans d'expérience dans une organisation de cybersécurité de premier plan, dans les domaines de la détection des menaces, de la réponse aux incidents et de la stratégie de sécurité. Travaillant en étroite collaboration avec le PDG, l'approche de Deterding en matière de réduction des risques consiste à se concentrer sur les actions les plus simples mais les plus percutantes, et ce, le plus tôt possible, pour « attraper les attaquants au début de la chaîne d'attaque. » Pour toute organisation, suggère Deterding, cela devrait commencer par l'authentification multi-facteurs (MFA).

Afni faisait déjà beaucoup de choses excellentes dans son programme de sécurité, notamment le déploiement de l'MFA pour la quasi-totalité de ses 10 000 employés à travers le monde—mais les attaques par phishing ciblées restaient un problème. Au cours de ses trois premières semaines chez Afni, Deterding a donné la priorité à l'adoption de l'MFA à 100 %. Ensuite, Deterding a ciblé le remplacement des méthodes d'authentification classiques.

L'authentification classique telle que l'authentification multi-facteurs mobile introduit des risques lorsque les utilisateurs prennent l'habitude d'appuyer sur « approuver » pour chaque demande d'authentification (fatigue MFA) ou sont victimes d'attaques par phishing de type « attaquant au milieu » (AITM). Cependant, la faute de ces risques ne revient pas à l'utilisateur, mais à l'authentification classique. Au moment de remplacer l'authentification classique, Afni savait que les clés de sécurité offraient une MFA résistant au phishing — et étaient insensibles aux attaques où les attaquants interceptent ou incitent les utilisateurs à révéler des informations.



**Brent Deterding**  
RSSI, Afni

« L'authentification multi-facteurs est l'un des moyens les plus rentables de réduire considérablement les risques, » note Deterding, « Réduire les risques face à des adversaires sophistiqués, bien coordonnés et déterminés, le MFA résistant au phishing en particulier est essentiel. »



Une clé de sécurité est la « référence absolue » en matière d'authentification, quelque chose que vous possédez physiquement. Pour moi, la YubiKey était le seul choix. Je n'ai pas cherché ailleurs. »

Brent Deterding, RSSI, Afni



La YubiKey est une clé de sécurité matérielle moderne basée sur FIDO qui permet l'authentification multi-facteurs (MFA) résistant au phishing et l'authentification sans mot de passe à grande échelle. En tant que seule solution éprouvée pour stopper 100 % des piratages de compte dans des recherches indépendantes, la YubiKey offre une authentification forte avec une expérience utilisateur rapide et facile, et répond aux besoins de conformité des données hautement réglementées. De plus, la YubiKey réduit les risques associés aux nouvelles méthodes de travail qui impliquent des environnements de travail à distance ou hybrides.

« Chaque utilisateur ayant une YubiKey, je n'ai pas à m'inquiéter de la fuite d'informations d'identification, » poursuit Deterding. « C'est une très, très bonne situation pour un RSSI. »

## Répondre aux nouvelles exigences en matière de cyberassurance de manière rentable avec les YubiKeys

Un facteur clé pour Afni dans l'adoption du MFA résistant au phishing avec les YubiKeys a été l'évolution du paysage de la cyberassurance et de ses exigences. L'augmentation du volume et de la gravité des incidents de cybersécurité a entraîné une augmentation des primes de cyberassurance, ainsi que de nouvelles sous-limites et exclusions. Alors que les assureurs tentaient de mieux quantifier et contrôler les pertes, les mots de passe n'étaient plus acceptables pour être éligible à la cyberassurance. De plus en plus, dépasser les mots de passe pour adopter le MFA est devenu la norme pour être éligible à la cyberassurance.

Lors de la soumission pour le renouvellement de la cyberassurance, Deterding a préparé une présentation pour un groupe d'assureurs qui a brossé un nouveau tableau des risques chez Afni. Il y a énuméré la couverture MFA à 100 %, la modernisation du MFA avec des YubiKeys pour 100 % des employés, la gestion de la posture des appareils à 100 % grâce à l'accès aux points de terminaison Microsoft, la couverture de détection et de réponse des points de terminaison à 100 %, et toutes les vulnérabilités externes corrigées dans les 72 heures—les quatre piliers du programme complet de Deterding pour « attraper les attaquants de bonne heure. » Bien qu'il ne s'agisse pas d'une représentation complète de tous les efforts d'Afni, ces quatre piliers ont démontré une réduction complète des risques.

Dans un marché où les primes sont en hausse, Afni a non seulement obtenu une couverture, mais les assureurs étaient également prêts à rivaliser sur les prix. « Au final, Afni a bénéficié d'une assurance avec une réduction de 30 % par rapport à son niveau précédent. Quand je descends d'un tiers et que d'autres montent de 20 % ou plus, c'est une très grande victoire, » note Deterding. « En fait, j'estime que nos primes représentent presque la moitié de ce que les autres doivent payer. »

## Adoption accélérée de l'authentification multi-facteurs (MFA) résistant au phishing à grande échelle avec YubiKeys as a Service

L'impératif de l'authentification multi-facteurs (MFA) résistant au phishing avec les YubiKeys était clair. Par conséquent, Afni a élaboré une stratégie de déploiement efficace pour assurer le succès de l'entreprise et de ses utilisateurs. Elle a choisi d'échelonner le déploiement de ses YubiKeys, d'abord auprès des employés ayant accès aux solutions Microsoft ou un accès privilégié aux systèmes et aux données clients, puis de l'étendre à ses agents de centres d'appel mondiaux.

Avec un réseau mondial de centres d'opérations et une large main-d'œuvre à distance, Afni souhaitait la flexibilité de YubiEnterprise Subscription, un modèle d'abonnement YubiKey as a Service qui réduit le coût initial, augmente la flexibilité et aide à accélérer les déploiements prévus. Grâce aux droits pour des clés de remplacement pour couvrir le taux de désabonnement et le modèle d'abonnement à faible coût, Afni peut rester agile pour gérer le rotation du personnel ou les clés perdues/volées sans aucun suivi de série fastidieux.

Du début à la fin, l'objectif était d'expédier et d'inscrire des YubiKey 5C NFC aux deux groupes d'utilisateurs, le premier groupe d'ici la fin 2022 et la deuxième phase en 2023. La première phase de déploiement a permis d'affiner les processus et d'aplanir les difficultés liées à la distribution, la formation des utilisateurs, l'inscription des clés et l'utilisation. Le retour positif a permis une large adoption par les utilisateurs.

Pour rester sur le thème de la « facilité », l'intégration des employés a non seulement mis en avant les avantages de la YubiKey en matière de sécurité, ou le fait que les méthodes d'authentification classiques seraient progressivement éliminées, mais aussi que le travail serait plus rapide et plus facile. « Au lieu d'un long mot de passe que vous oubliez parfois, vous tapez un code PIN à quatre chiffres et vous touchez la YubiKey, » explique Deterding, « C'est rapide et facile. Le retour est très positif. »



Au final, Afni a bénéficié d'une assurance avec une réduction de 30 % par rapport à son niveau précédent. Quand je descends d'un tiers et que d'autres montent de 20 % ou plus, c'est une très grande victoire, » note Deterding. « En fait, j'estime que nos primes représentent presque la moitié de ce que les autres doivent payer. »

Brent Deterding, RSSI, Afni



Je suis entièrement favorable à ce que l'adoption de la technologie soit aussi simple que possible. Si je peux appuyer sur le bouton « Facile » en utilisant des YubiKeys et aussi leur modèle d'abonnement pour m'assurer que tous mes utilisateurs ont des YubiKeys, c'est une grande victoire pour moi ! »

Brent Deterding, RSSI, Afni



Nous suivons le même chemin que les organisations les plus avancées au monde. Et nous sommes tous en train de déployer des YubiKeys. »

Mike Schwermin, DSI, Afni

À l'avenir, Afni espère améliorer encore l'expérience des employés en supprimant la nécessité de changer les mots de passe des applications ou en supprimant complètement les mots de passe. De plus, chaque employé est encouragé à utiliser sa YubiKey pour ses comptes personnels afin de l'aider à développer des habitudes sécurisées et à améliorer l'image de l'entreprise. « Nous aidons les employés à être plus en sécurité dans leur vie personnelle ainsi qu'au travail, ce qui profite à tout le monde. »

Les avantages de YubiEnterprise Subscription étaient logiques pour Deterding, car il examinait les taux de rotation de ses employés de production, qui s'occupaient principalement des clients dans les centres d'appel du monde entier. « Je suis habitué aux offres d'abonnement dans le cloud et YubiEnterprise Subscription présente des avantages utiles qui correspondaient parfaitement à nos besoins. »

### Microsoft et YubiKeys fonctionnent ensemble de manière transparente pour renforcer les politiques de sécurité

La YubiKey est prise en charge de manière native par Microsoft, permettant un accès facile et sécurisé à OneDrive, SharePoint et Office365 pour tous les employés de bureau hors production. La YubiKey sécurise également l'accès à distance avec l'authentification multi-facteurs (MFA) résistant au phishing pour les travailleurs à distance utilisant un VPN.

Après l'effort visant à amener les utilisateurs au-delà des mots de passe vers le MFA, et à élever le niveau de sécurité avec une MFA 100 % résistant au phishing avec la YubiKey, l'étape suivante pour Afni a été d'appliquer de nouvelles normes MFA en dépréciant l'authentification classique et en autorisant uniquement les YubiKeys. Afni a tiré parti des nouvelles fonctionnalités d'accès conditionnel de Microsoft Azure AD pour appliquer l'utilisation des YubiKeys pour toutes les applications requises. Deterding a partagé une leçon apprise : il aurait dû forcer l'utilisation des utilisateurs YubiKey enregistrés dès le départ, plutôt que de prévoir une période de transition.



Le fait que je puisse assurer l'identité avec une YubiKey physique, même pour les travailleurs à distance, est très bénéfique pour mes efforts de réduction des risques chez Afni. »

Brent Deterding, RSSI, Afni

### Soutien de la direction et partenaire de confiance

La vision de Deterding n'aurait pas été possible sans une large adhésion de la direction, en particulier avec le DSI d'Afni, Mike Schwermin. Mike est un vétéran de 20 ans dans l'industrie BPO et un leader reconnu dans la fourniture de solutions de nouvelle génération pour Afni. « Je suis reconnaissant pour le soutien extraordinaire de notre équipe de direction à nos efforts pour accroître notre cybersécurité. Mike et moi sommes en phase pour permettre à Afni de renforcer nos pratiques de sécurité. »

Prendre sa sécurité au sérieux et être transparent sur ses pratiques de sécurité a contribué à établir Afni comme un partenaire de confiance dans la chaîne d'approvisionnement. De plus, Afni a découvert qu'elle avait la même feuille de route que beaucoup de ses clients de centres d'appel qui déployaient déjà des YubiKeys.



En savoir plus  
[yubi.co/customers](https://yubi.co/customers)

[yubi.co/contacts](https://yubi.co/contacts)

À propos de Yubico En tant qu'inventeur de la YubiKey, Yubico facilite la connexion sécurisée. En tant que leader dans l'établissement de normes mondiales pour l'accès sécurisé aux ordinateurs, appareils mobiles et plus encore,

Yubico est également un créateur et contributeur clé aux normes d'authentification ouvertes FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F). Pour plus d'informations, veuillez consulter: [www.yubico.com](https://www.yubico.com).