CLOUDFLARE

DOSSIER DE SOLUTION

# Comment une authentification forte contribue au blocage des attaques par phishing

Les clés de sécurité et le modèle Zero Trust peuvent contrer les hameçonneurs

## La menace que fait peser le phishing

### Perte de données, réseaux compromis, vol de comptes

Les attaques par phishing ciblé sont l'un des vecteurs de menace les plus dangereux auxquels sont confrontées aujourd'hui les organisations. Les attaques par phishing et ingénierie sociale consistent à manipuler des personnes pour qu'elles divulguent leurs informations sensibles ou leur autorisation d'accès. Les identifiants de connexion sont des cibles courantes.

Lorsqu'elles aboutissent, les attaques de cette nature peuvent se traduire par :

- Prise de contrôle de comptes
- Un lien dans une attaque plus grande sur la chaîne d'approvisionnement
- L'exfiltration de données telles que des PII ou une adresse IP
- Des attaques par des logiciels malveillants tels que des rançongiciels

Fort heureusement, il existe des solutions hautement efficaces pour réduire le risque de phishing. Une de plus importantes est celle de l'authentification multifacteur (MFA)

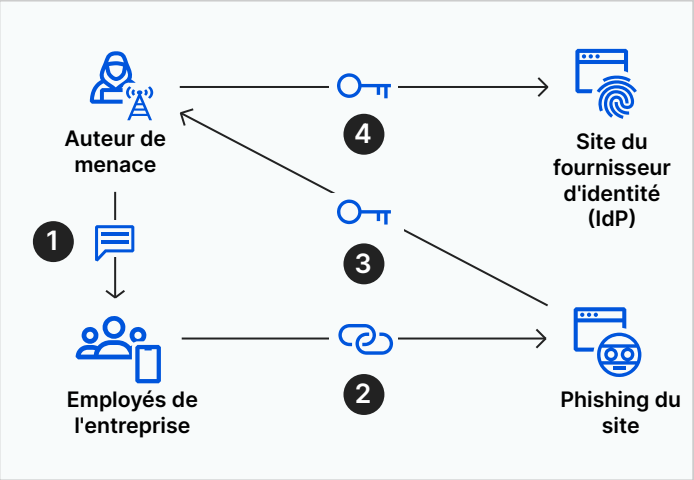



**Figure 1 :** Représentation graphique de l'organisation d'une attaque par phishing sur SMS. 1. Un message textuel qui semble légitime est envoyé. 2. Lien vers un site en apparence légitime. 3. En temps réel, les identifiants de la victime et le mot de passe limité dans le temps sont transmis. 4. Connexion au vrai site du fournisseur d'identité de l'entreprise.

## Comment l'authentification multifacteur (MFA) contribue au blocage de l'hameçonnage

### La MFA neutralise le vol de mot de passe

La MFA (Authentification multifacteur) exige des utilisateurs qu'ils présentent une clé en plus de leur nom d'utilisateur et du mot de passe lorsqu'ils se connectent. Sans cette clé, ils ne peuvent pas accéder à leurs comptes et il en va de même pour un attaquant.

### MFA avec clés logicielles

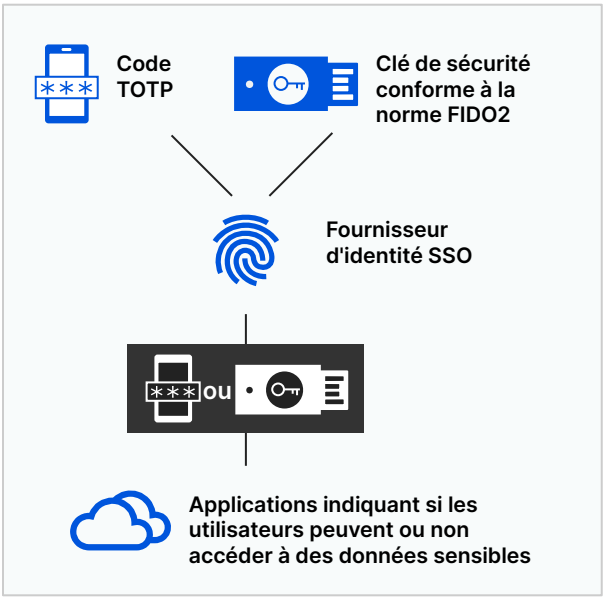
Le plus souvent la MFA se fait à l'aide de clés logicielles telles que des mots de passe à usage unique limités dans le temps. Ces mots de passe sont généralement transmis par message SMS, par e-mail ou par des applications. Si elles sont plus sécurisées que l'authentification à facteur unique, les clés logicielles peuvent être interceptées par des attaquants.

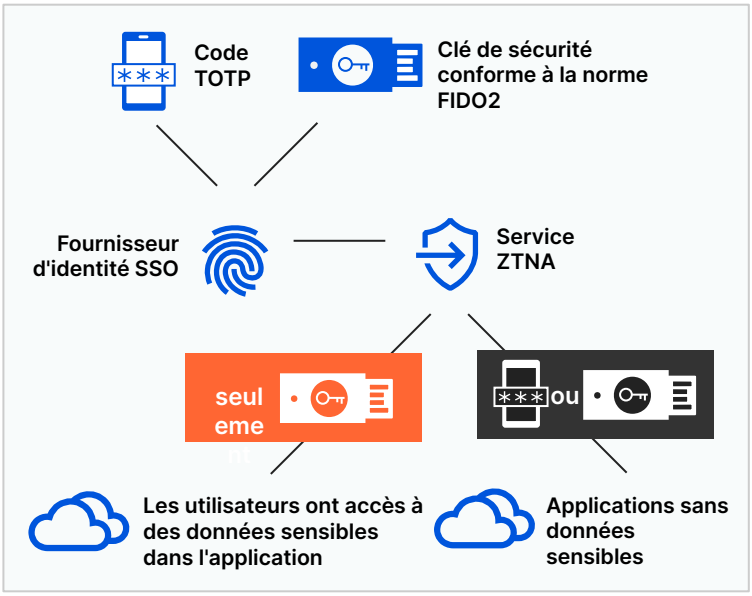
### MFA avec clés de sécurité

Les clés de sécurité conformes à la norme FIDO2, une fois émises, ne peuvent pas être interceptées par un attaquant et sont quasiment impossibles à voler sans accès physique. D'après Research by Google les clés de sécurité conformes à la norme FIDO2/U2F ont bloqué 100 % des tentatives d'usurpation de compte.[1]

## Appliquer de manière sélective une authentification forte

Certaines solutions IAM peuvent prendre en charge une authentification forte mais elles n'autorisent pas obligatoirement les administrateurs à réellement les exiger. Avec le modèle ZNTA vous pouvez faire en sorte qu'une authentification FIDO2 soit obligatoire, en particulier pour les applications comportant des données sensibles. Cloudflare exige une authentification multifacteur avec clé de sécurité pour chaque authentification, qui a fortement élevé notre niveau de sécurité.

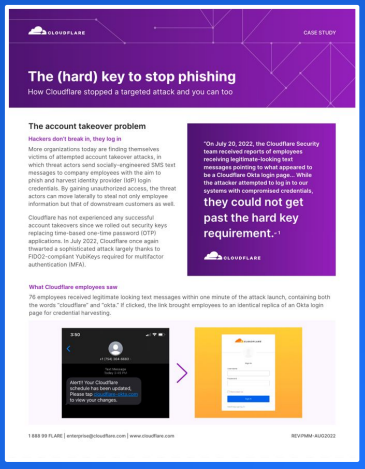



« Le 20 juillet 2022, l'équipe de sécurité de Cloudflare a reçu des rapports indiquant que des employés recevaient des messages textuels en apparence légitimes qui pointaient vers ce qui semblait être une page de connexion Cloudflare Okta...Lorsque l'attaquant tentait de se connecter à nos systèmes avec des identifiants compromis,

**il ne parvenait pas à répondre aux exigences de clé physique.** »[2]

CLOUDFLARE



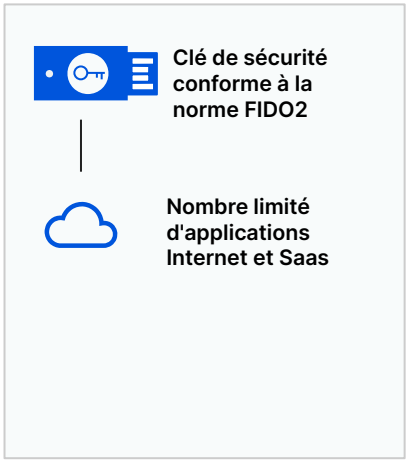
# Déployez une authentification forte partout

### MFA conforme à FIDO2 pour toutes vos applications

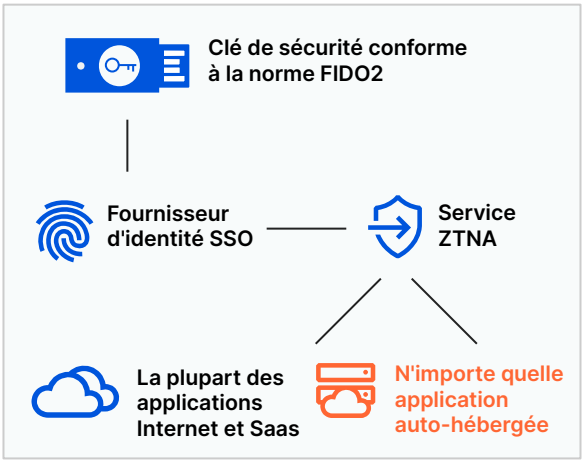
L'application de la MFA pour tous les services cloud est possible de plusieurs manières conventionnelles, en particulier lorsqu'un service d'authentification unique (SSO) est utilisé. Mais cela peut s'avérer difficile avec des applications existantes ou non web, parmi lesquelles de nombreuses ne prennent pas en charge ce type d'authentification nativement.

### Simplifiez le déploiement avec le ZTNA

Le modèle ZTNA (Zero Trust Network Access) agit comme une couche de regroupement autour de toutes vos ressources et permet d'appliquer des politiques d'authentification strictes pour chacune. Les applications Saas, auto-hébergées et non web peuvent être protégées par un modèle ZTNA qui facilite une authentification forte à appliquer dans toutes les applications.








## Points à retenir pour les organisations qui mettent en œuvre une authentification forte

**1**

### Centralisez votre IAM

Centralisez la gestion des identités et des accès (IAM) de sorte que la MFA soit plus simple à mettre en œuvre au travers de toutes les applications.

**2**

### Appliquer la MFA de manière sélective

Définir les options d'application sélective de la MFA (TOTP et FIDO2 ou FIDO2 uniquement) en fonction de l'identité et le contexte.

**3**

### Prenez en charge les appareils mobiles

Mettez en place des solutions FIDO2 pour les ordinateurs portables, les postes fixes et les serveurs, ainsi que les appareils mobiles

## Accélérez votre feuille de route Zero Trust

Demander un atelier sur l'architecture

Vous n'êtes pas encore prêts pour votre évaluation ?

Demandez un essai gratuit.

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. Article de blog Cloudflare, 9 août 2022, « Les rouages d'une opération de phishing sophistiquée et la manière dont nous l'avons arrêtée », blog.cloudflare.com/2022-07-sms-phishing-attacks/