SOLUTION BRIEF

How strong authentication helps stop phishing attacks

Security keys and a Zero Trust approach can thwart phishers

The threat posed by phishing

Lost data, compromised networks, stolen accounts

Targeted phishing attacks are one of the most dangerous threat vectors organizations face today. Phishing and social engineering attacks aim to manipulate people into giving up sensitive information or access. Login credentials are common targets.

Successful attacks of this nature can result in:

- Account takeover
- A link in a bigger supply chain attack
- Data exfiltration such as PII and IP
- Malware attacks such as ransomware

Fortunately, there are highly effective solutions available to reduce the risk of phishing. One of the most important is multi-factor authentication (MFA).

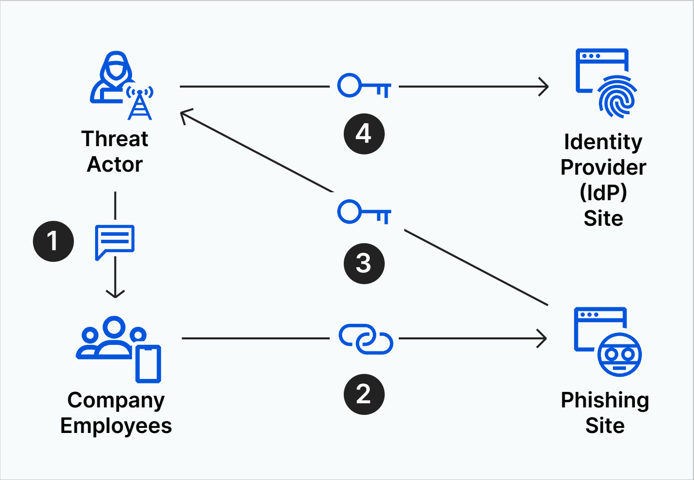


Figure 1: Anatomy of an SMS phishing attack. 1. Legitimate-looking text message sent. 2. Linked to legitimate-looking site. 3. In real-time, victim's credentials and time-based one-time passcode relayed. 4. Logs into real company IdP site.

How multi-factor authentication (MFA) helps stop phishing

MFA neutralizes password theft

MFA requires users to present a key in addition to their username and password when logging in. Without this key, they cannot access their accounts, and neither can an attacker.

MFA with soft keys

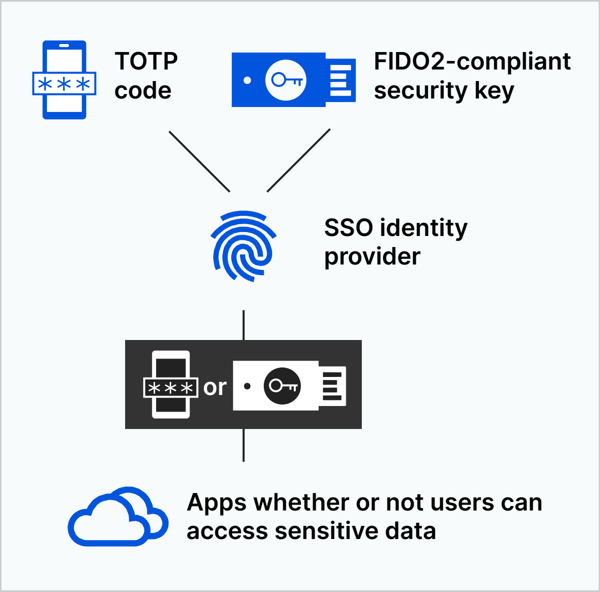
A common implementation of MFA is to use soft keys such as time-based one-time passcodes (TOTPs). TOTPs are often issued via SMS message, email, or apps. While more secure than single-factor authentication, soft keys can be intercepted by attackers.

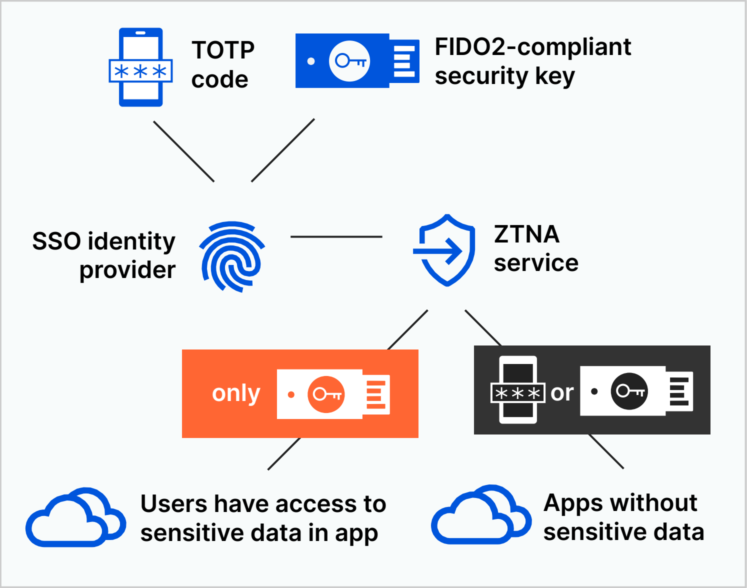
MFA with security keys

FIDO2-compliant security keys, once issued, cannot be intercepted by an attacker and are nearly impossible to steal without physical access. Research by Google found that the use of FIDO2/U2F-compliant security keys blocked 100% of account takeover attempts.[1]

Selectively enforce strong authentication

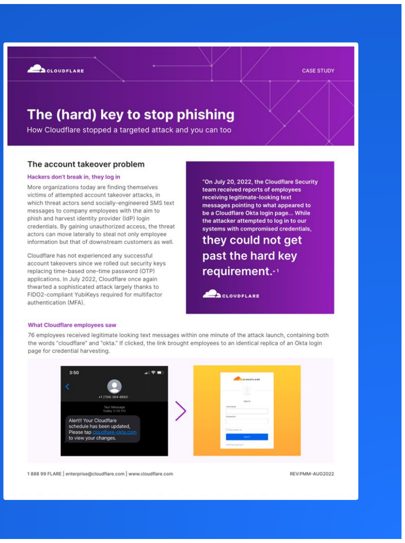
Some IAM solutions may support strong authentication but may not allow admins to truly require it. Using ZTNA, you can ensure FIDO2 authentication is required especially for apps housing sensitive data. Cloudflare requires security key MFA for every authentication, which has heavily strengthened our security posture.


TOTP code
FIDO2-compliant security key
SSO identity provider
or
Apps whether or not users can access sensitive data


TOTP code
FIDO2-compliant security key
SSO identity provider
ZTNA service
only
or
Users have access to sensitive data in app
Apps without sensitive data

> "On July 20, 2022, the Cloudflare Security team received reports of employees receiving legitimate-looking text messages pointing to what appeared to be a Cloudflare Okta login page... While the attacker attempted to log in to our systems with compromised credentials,
>
> **they could not get past the hard key requirement."** [2]

CLOUDFLARE


CLOUDFLARE

CASE STUDY

The (hard) key to stop phishing

How Cloudflare stopped a targeted attack and you can too

The account takeover problem

Hackers don't break in, they log in

More organizations today are finding themselves victims of attempted account takeover attacks, in which threat actors send socially-engineered SMS text messages to company employees with the aim to phish and harvest identity provider (IdP) login credentials. By gaining unauthorized access, the threat actors can move laterally to steal not only employee information but that of downstream customers as well.

Cloudflare has not experienced any successful account takeovers since we rolled out security keys replacing time-based one-time password (OTP) applications. In July 2022, Cloudflare once again thwarted a sophisticated attack largely thanks to FIDO2-compliant YubiKeys required for multifactor authentication (MFA).

"On July 20, 2022, the Cloudflare Security team received reports of employees receiving legitimate-looking text messages pointing to what appeared to be a Cloudflare Okta login page... While the attacker attempted to log in to our systems with compromised credentials, they could not get past the hard key requirement." [1]

CLOUDFLARE

What Cloudflare employees saw

76 employees received legitimate looking text messages within one minute of the attack launch, containing both the words "cloudflare" and "okta." If clicked, the link brought employees to an identical replica of an Okta login page for credential harvesting.

3:50

+1 (754) 364-6683

Text Message
Today 3:49 PM

Alert!! Your Cloudflare schedule has been updated, Please tap cloudflare-okta.com to view your changes.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:PMM-AUG2022

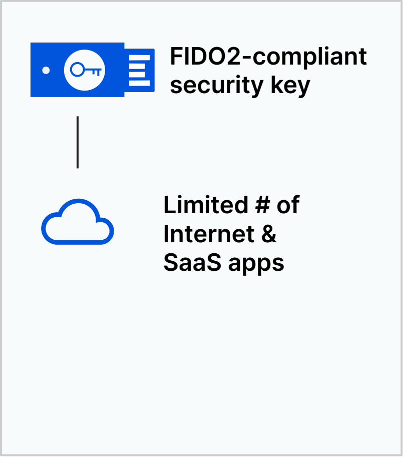
Roll out strong authentication everywhere

FIDO2-compliant MFA for all your apps

Enforcing MFA for cloud services is possible in a variety of conventional ways, particularly when a single sign-on (SSO) service is used. But this can be difficult with legacy or non-web apps, many of which do not support this kind of authentication natively.

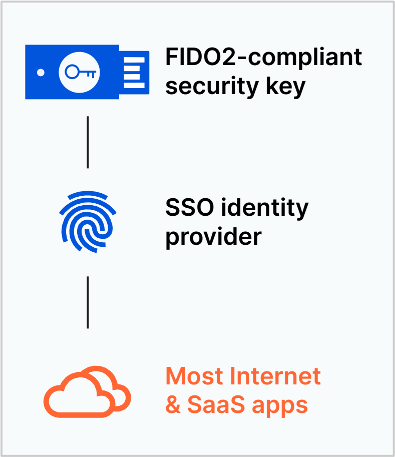
Simplify rollout with ZTNA

Zero Trust Network Access (ZTNA) acts as an aggregation layer around all your resources and enables strict authentication policies for each of them. SaaS, self-hosted, and non-web applications alike can sit behind ZTNA, which makes strong authentication easier to enforce across all applications.



FIDO2-compliant security key

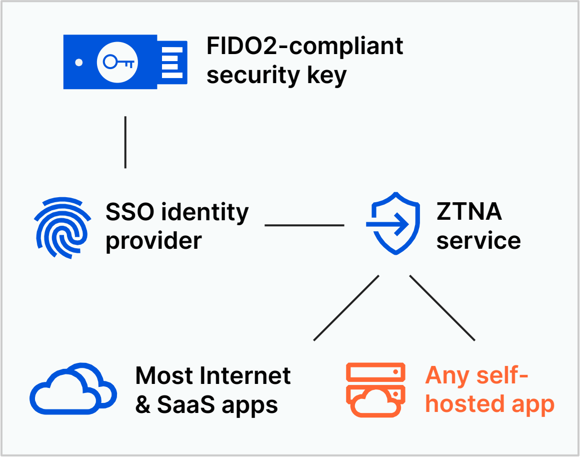
Limited # of Internet & SaaS apps



FIDO2-compliant security key

SSO identity provider

Most Internet & SaaS apps



FIDO2-compliant security key

SSO identity provider

ZTNA service

Most Internet & SaaS apps

Any self-hosted app

Key takeaways for organizations implementing strong authentication

1

Centralize your IAM

Centralize identity and access management (IAM) so that MFA is simpler to implement across all apps.

2

Enforce MFA selectively

Establish selective enforcement of MFA options — TOTP and FIDO2 or FIDO2 only — based on identity and context.

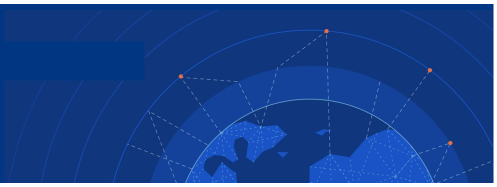
3

Support mobile devices

Issue FIDO2 solutions for laptops, desktop computers, and servers, as well as mobile devices.

Accelerate your Zero Trust roadmap

Request an architecture workshop



Not ready for your assessment?

Request a free trial.

[1] krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/

[2] Cloudflare blog post, August 9, 2022, "The mechanics of a sophisticated phishing scam and how we stopped it", blog.cloudflare.com/2022-07-sms-phishing-attacks/