Cloudflare embraces FIDO to help improve its own security

THE CHALLENGE:
Improving Employee Access with Zero Trust

When Cloudflare started the company provided its employees with access to internal applications via a virtual private network (VPN). Access to some, but not all applications behind the VPN required two factor authentication, typically done with One Time Passcodes (OTP) generated by applications like Authy or Google Authenticator.

Cloudflare realized that it needed a more secure and scalable approach than VPN and started a process of moving toward a Zero Trust architecture utilizing Cloudflare Access.

From OTP to unphishable FIDO authentication

As part of its migration to a zero trust architecture, starting in 2018 Cloudflare began its usage of FIDO based security keys.

The goal behind using FIDO2 was to provide strong authentication that would enable Cloudflare's zero trust model.

> ***"I wanted something that was unphishable," said Derek Pitts, director of enterprise security at Cloudflare. "If we were going to go through all the trouble of redoing a lot of our identity and access management infrastructure, I wanted it to be future proof and resilient."***

Overview

CLOUDFLARE

Founded in 2010, Cloudflare is one of the world's leading internet content delivery and security platforms.

Overview:

Cloudflare is one of the world's most deployed security and content delivery platforms. Cloudflare's products include a range of services including web performance, application network, zero trust and developer services.

Cloudflare's network handles over 36 million HTTP requests per second and blocks over 124 billion cyber attacks a day. The Cloudflare network has over 200 points of presence around the globe.

Overcoming barriers to adoption with selective enforcement

Cloudflare's path to adoption of FIDO security keys was not an entirely straight path. Initially there were concerns around account recovery and replacement of lost physical security keys.

Another challenge was the fact that Cloudflare's users were used to using OTP technology with Google Authenticator, or Authy. Managing user change aversion and education were key components in the switch from OTP to FIDO security keys. This led Cloudflare to a selective enforcement approach, so as not to force change on users that could potentially lock them out.

What Cloudflare did was to integrate FIDO into its access identity aware proxy that internal users used to access internal sites. Instead of immediately requiring FIDO for all internal sites, Cloudflare initially only required the use of security keys on three of its sites. Selective enforcement for FIDO security keys were activated on July 20, 2020, which is the day Twitter fell victim to a social engineering attack.

"That day was mayhem and we wanted to ensure that didn't happen to us," Pitts said.

Pitts said that by requiring the use of FIDO2/WebAuthn for its three more most sensitive internal apps, adoption grew as it gave employees a training ground to get familiar with the technology. In 2021, Cloudflare made the switch to requiring FIDO security keys across its network.

LESSONS LEARNED: Take the small wins where you can

From the outset, the movement toward strong authentication had top down support from Cloudflare's CEO, CIO and CSO. Pitts said that having the executive buy in was important as it helped his team to push through when it ran into issues.

Cloudflare has a large and complex network architecture and it didn't move to WebAuth/FIDO2 overnight. Pitts said that it was a multi-year effort that was successful on the foundation of a series of incremental small wins that helped to prove that the technology can work to improve security.

The small wins approach incorporated Cloudflare's selective enforcement approach. Pitts said that it's important to have a training ground that will allow users to try out security keys and get familiar with the approach.

Selective enforcement ended up being a huge deal for us," Pitts said. "That was one of the biggest forcing functions and things that made this project successful."

Read Cloudflare's blog, "How Cloudflare implemented hardware keys with FIDO2 and Zero Trust to prevent phishing," to learn more about their FIDO Authentication implementation.