Case Study

Challenge | Identity Fragmentation in the Enterprise

A leading North American financial institution had a large-scale initiative to simplify authentication for their employees, partners, contractors, and high net-worth clients. The IT org was required to support multiple Identity Providers, while more than 10,000 employees had to utilize 3 separate MFA apps in addition to 14-character complex passwords. What might cause such Identity Turmoil?

New Leadership can bring new strategic direction. Assume you have Okta deployed and are using Duo for 2-FA. Your new CIO is going all-in on Azure AD, bringing the Microsoft Authenticator app into the mix. Which MFA app is your primary login method? Are you going to switch employees from one app to another? Why is everyone still using passwords?

Mergers & Acquisitions introduce new Identity layers into an organization. Tying them together often requires significant time and effort and can create a fragmented environment for a team that is already juggling too many initiatives. Which identity platform is your source of truth? Who is the primary SSO? What about all the new customer identities that have been acquired?

Cloud and IT Strategy is constantly evolving and can push IAM in a whole new direction by introducing users to new products and processes. When IT strategy changes course, are you going to re-enroll the whole organization? Will this exercise be repeated upon similar circumstances?

Signs of Identity Turmoil

- MFA Fatigue
- User Disruption
- Reliance on Passwords
- MFA Gaps & Inconsistent Login Experiences

Solution | Unifiying Identity Experiences with True Passwordless SSO

This organization leveraged their cloud transformation budget to jumpstart their passwordless initiative. They focused on perfecting the authentication experience, leaving the IdP and SSO layer untouched. The result was a unified passwordless login across all identity products and services. Most importantly, users benefited from a passwordless login experience more than 300% faster than what they had before.

> The Benefit of Passwordless is Disrupting Authentication without Disrupting the User. - CISO

Fast, Consistent Login Experiences

They replaced 3 separate password-based MFA apps with a single Passwordless app. Users are able to enroll in a single authentication layer that secures all mobile, web, desktop and SSO login experiences. User login became faster, easier, and consistent.

Rapid Password Elimination

The IT team was able to accelerate the rollout of passwordless authentication. The organization eliminated passwords faster than they anticipated – and they did so without the pain of managing a crowd of fragmented MFA apps, flows, and experiences.

Future Proof Authentication

They were able to offset any user disruption by future-proofing the user authentication experience against the constantly evolving IT initiatives.