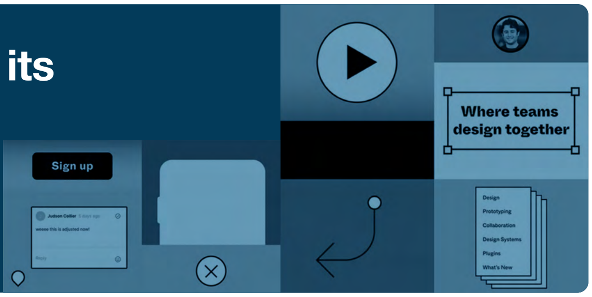
yubico

Figma implements strong security for all its employees with Okta and the YubiKey



Case Study

Figma

Industry
Technology and Design

Benefits

- Strong MFA for all users
- Improved user experience
- Scalable solution

Deployment info

- YubiKey 5Ci
- YubiEnterprise Delivery
- Type of users: All company employees
- Protocols: FIDO2/WebAuthn
- Technology partner: Okta

About Figma

Figma is a design platform for teams that build products together. With its cloud-based screen design tool, teams achieve a shared understanding around design without worrying about syncing, exporting or installing software. Figma has simplified collaboration across the entire design process for thousands of companies and millions of users, including designers, developers, product managers, marketers and others.

The challenge: Figma enforces a new security paradigm

In the last quarter of 2020, Figma looked for ways to implement strong authentication protection against potential phishing attacks for remote employees. Figma uses Okta as its identity provider (IdP). After a careful consideration of all the authentication methods available in Okta Adaptive MFA, Figma landed on FIDO2/WebAuthn as the only method to prevent account takeovers at scale.

Figma's Head of Security, Devdatta Akhawe, wanted a solution that was easy to use, created minimal friction, and worked across all employees' modern devices. He also wanted to ensure a smooth transition, with a seamless implementation that caused very little disruption to company workflows. It helped make the case to leadership and, most critically, top IT staff, that WebAuthn now has broad support among IAM providers, hardware and software makers.

Akhawe also had to deal with the new, pandemic-induced work environment. How would remote employees receive their YubiKeys? When employees are scattered geographically, engineering an efficient and safe delivery system for the keys would be a challenge.

The solution: The YubiKey 5Ci and YubiEnterprise Delivery (YED) meet the challenge

The YubiKey is FIDO2/WebAuthn compliant and already integrates seamlessly with Okta Adaptive MFA. Among the different form factors, the YubiKey 5Ci was selected because of its versatility and dual connector (Lightning for iOS devices and USB-C for Mac and Android devices).

The YubiEnterprise Delivery (YED) solution from Yubico handled the logistics of sending keys to remote employees, simplifying the procurement process and generating a single invoice for Figma to handle. This turned out to be a huge time saver and, given COVID-19 restrictions, would have been impossible for Figma to carry out on its own.

> "I recommend signing up for YubiEnterprise Delivery, Yubico's service that ships YubiKeys to your employees anywhere in the world while giving you and your finance team a single invoice."
>
> **—Devdatta Akhawe, Head of Security, Figma**

Case Study

Figma

Industry

Technology and Design

Benefits

- Strong MFA for all users
- Improved user experience
- Scalable solution

Deployment info

- YubiKey 5Ci
- YubiEnterprise Delivery
- Type of users: All company employees
- Protocols: FIDO2/WebAuthn
- Technology partner: Okta

The YubiKey integration with Okta gave Figma the ability to set security by risk level. Users were required to use FIDO2/WebAuthn when accessing critical-risk applications like AWS, but during the transition these users could still log in without a FIDO device for less critical pathways. Users were permitted to voluntarily self-register their FIDO security keys, which is a simple and fast process that happens in minutes.

“The nice thing about Okta and the YubiKey combination is the flexible configuration options it provides. We started small, requiring FIDO2 on only a few applications, but very quickly we expanded to all applications for employees in critical risk functions,” said Devdatta Akhawe, Figma’s Head of Security.

The transition to FIDO-only authentication was possible because of YED’s flexibility and YubiKey’s simple integration with Okta. During the transition, communication was key to getting users to 100 percent rollout. Management spread the word through internal channels that every employee needed to register at least one YubiKey. Yubico communicated with users via Slack and monitored logs to make sure that eventually everyone did get correctly registered. When the user base got to full registration, Figma only had to “flip the switch” to go to an all-FIDO system.

The implementation was done incrementally to ease users into it. For example, at first YubiKeys were only required during working hours, but as employees grew accustomed to the new system, that was extended to a 24-7 requirement.

> “The nice thing about Okta and the YubiKey is all the configuration options it provides. We started with requiring FIDO2 while accessing certain high-risk applications, and we soon expanded to all applications for employees in critical risk functions, so that the YubiKey was the only authentication method allowed.”
>
> **—Devdatta Akhawe, Head of Security, Figma**

The results: Figma enhances security with a company-wide deployment in a matter of weeks

Remote workers now have the strongest level of protection against phishing attacks, and the rollout was efficiently completed company-wide. As he was planning implementation, Akhawe was concerned about implementing strong authentication on mobile devices. But the YubiKey 5Ci has proven itself in the field by being compatible with both iOS and Android devices. Users have appreciated the convenience of using their YubiKey only once upfront during registration. Essentially, if they self-register the key through their computers initially, and then activate it on a FaceID-enabled phone, FaceID can be used going forward for quick mobile authentication.

The delivery service included in YED was crucial to the success of the rollout, getting YubiKeys quickly into the hands of 250 users, no matter where they were, and providing easy self-registration instructions.

The security team at Figma could rest easy now that strong authentication was the norm in the company culture. Akhawe appreciated the focus Figma’s top leadership put on upgrading security and reported back that the implementation had been carried out with very few bumps along the way, and in record time. Most importantly, Figma employees now carry and use their YubiKey 5Ci on a daily basis and are protected against external malicious attacks.

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088