yubico

CASE STUDY

Industry

Security

At a glance

1+ million users

20+ global locations

2+ petabytes of protected data

Key results

Streamlined onboarding and distribution of YubiKeys at scale

Simplified employee experience

Preparation for a passwordless future

Protocols

WebAuthn/FIDO2

Yubico solutions deployed

YubiKey 5C NFC

YubiKey 5 NFC

A global provider of MSP-delivered IT solutions on journey to passwordless with YubiKeys

Phishing awareness program identifies the need for modern phishing-resistant multi-factor authentication (MFA)

A global provider of security and cloud-based solutions purpose-built for Managed Service Providers (MSPs) has a toolbox of different products to help protect small and medium businesses (SMBs) against threats and to minimize downtime—including tools in data backup and recovery, network management and automations for business operations. To date, there are over one million users across more than 20 global locations.

The organization's Director of IT is responsible for all the internal employee-facing systems and an employee's digital experience within the organization. He oversees employee onboarding and device provisioning, support infrastructure, collaboration products and the controls used to manage these systems, including endpoint security, identity access management, and authentication. As part of the IT team's regular collaboration with the CISO and InfoSec team to identify gaps in control sets, they realized they needed a higher assurance authenticator to protect employees against phishing attacks. The team was aware that it was possible for user credentials to be compromised by phishing and multi-factor authentication (MFA) fatigue, a situation that occurs when an employee is repeatedly asked for login verifications, inadvertently approving a malicious push request.

"Managing against the global threat landscape is about the employee," notes the Director of IT. "How do we protect our employees? How do we enable them to work, but also be secure and prevent them from being phished or having their credentials exposed or authenticating to something they don't mean to?" These questions required more than just employee training and awareness—it required an MFA solution that would be phishing-resistant.

> "Some of our biggest concerns are around the impact to the business if employees do release their credentials or if the credentials are exposed or if a phishing attempt is successful."
>
> **Director of IT**

> Second factor is a big concern of ours. Once we saw the light with WebAuthn, we said yes - let's get everybody a YubiKey."
>
> **Director of IT**

Armed with the knowledge that many data breaches are tied to credentials, the organization's security training includes mock phishing emails that educate employees if they click on bait emails. To test the effectiveness of its existing two-factor authentication program, which included a one-time password (OTP) sent by push notification to a mobile device, the team created a fake website to mimic a man-in-the-middle (MiTM) attack. In this kind of attack, a malicious website is created to look like original sites and manipulate users into entering login credentials or two-factor authentication (2FA) security codes. The organization created its own MiTM attack that sent a calendar invite using an internally-created "malicious" video conference URL that led to a website that mimicked its Okta single-sign on (SSO) landing page. At this stage, the program would trigger a push 2FA code.

The phishing awareness program was sent to 200 employees, about 40% of whom entered their credentials into the false SSO landing page and 40% accepted the 2FA push. If this had been a real attack, an attacker would have compromised 40% of employee credentials and have full use of those credentials to access internal systems for seven days, based on internal policy. The phishing awareness program highlighted common challenges associated with mobile-based authenticators such as SMS OTP, which research has indicated only blocks 76% of targeted attacks.

"Armed with that evidence," notes the Director of IT, "we knew we had to address this gap." Examining the latest technologies brought him to FIDO2 and WebAuthn, modern authentication protocols created by the FIDO Alliance. FIDO2 enables modern, possession-based credentialing that requires the use of either biometric information or security key to verify user identity—a process which is phishing-resistant. "Once we saw the light of WebAuthn, it was clear that was the next step we needed to take."

Phishing-resistant YubiKey delivers strong identity assurance for access to Okta

At the time of the social experiment, the organization was managing identity access with Okta—using two-factor authentication with SMS OTP to gain federated access to a portal of employee-facing apps and services. For privileged engineers and for users who either can't, won't or don't use mobile-based MFA, the organization had already found Yubico's hardware security key, the YubiKey, to act as a strong second factor. Over 100 users were already leveraging the YubiKey as a second factor or to generate 2-step verification codes.

As a multi-protocol security key, the YubiKey was already FIDO2 compliant and could integrate seamlessly with Okta, giving the organization a head start on its path to highest assurance authentication. "When we started exploring the different phishing methodologies that came up, and how to protect against them, we discovered FIDO2," the Director of IT explains. "Already having the YubiKeys in our environment and being able to enroll them as FIDO2 compliant helped pave the way for us to expand YubiKeys to the rest of the organization."

> Compliance is on my radar. Although compliance is just two-factor in general, we hold ourselves compliant to the next iteration of that. Going to FIDO2 or WebAuthn is a notch above - the next step."
>
> **Director of IT**

The organization rolled out the YubiKey 5C NFC or 5 NFC to all 1,700+ employees, who at the time were working remotely during the pandemic. YubiKeys were distributed in batches of 200 per week, giving each group a one-week grace period to onboard, a process that took only “a matter of seconds” to make the YubiKey live. Once distribution was complete, the option to use OTP or 2FA second factors was eliminated, requiring the exclusive use of the YubiKey and WebAuthn standards to access Okta.

“We didn’t want people using OTP or 2FA second factors,” says the Director of IT. “So we derived policies within Okta to only allow the FIDO2 or biometric authenticators against certain applications within our Okta environment.”

YubiEnterprise Services and Okta workflows simplify deployment at scale

With the need to support the timely delivery of YubiKeys to its remote workforce using limited resources, the organization put together a deployment strategy that included Okta workflows YubiKey as a Service and YubiEnterprise Delivery. Based on the rate of employee turnover and the number of devices purchased within a year, having a predictable subscription spend made the most sense, particularly given the added flexibility to upgrade to the latest YubiKeys. YubiEnterprise Delivery not only got devices into the hands of a remote workforce, but also automated the fulfillment workflow.

> “The YubiEnterprise Delivery program went above and beyond for us. Finding out there was that API and we could automate fulfillment was great. The actual fulfillment and delivery of YubiKeys has been flawless.”
>
> **Director of IT**

The organization was able to integrate the YubiEnterprise Delivery API into an Okta workflow to automate communication with users and streamline workflows. Leveraging Okta workflows and an integration to Slack, they were able to query users based on their device and deployment group to verify the kind of YubiKey they would need (depending on device port) and their shipping address. Once the form was completed on Slack, it returned to the Okta workflow for the next batch order with YubiEnterprise Delivery. The system would further update the user when the YubiKey had shipped and, once delivered, with documentation to support enrollment.

“Employees would receive a notification that ‘Your YubiKey has been delivered, make sure you find it and enroll it,’” shares the Director of IT. “From that point, employees would have a seven-day grace period to enroll the device.” After the grace period, employees were moved into a different Okta group that would then enforce the security key requirement.

The existing relationship with YubiKey and the availability of YubiEnterprise Delivery “made us even more excited to move forward with all employees having YubiKeys,” says the Director of IT. By automating the bulk of this process, the organization only needed one engineer to roll out 200 YubiKeys every week until the entire organization was onboarded.

“From querying an employee and deciding what the user needed, all the way through ordering, shipping assets and enforcing the use of them, it was all within one workflow,” says the Director of IT. “From a fulfillment, delivery and enablement perspective, it was very smooth.”

One key, one streamlined workflow

The rollout included getting buy-in from executives, who were fully briefed on the results of the phishing experiment, the risks and the benefits of modern authentication standards. While the risks and benefits were clearly articulated, it was the convenience of the YubiKey that helped the deployment go smoothly at all levels of the organization. Research has indicated that authenticating with the YubiKey is up to four times faster than with SMS OTP. “Our executives were excited to have the YubiKey integrated into their workflows,” explains the Director of IT.

The change management strategy included clear, automated communication over Slack and articles on how to enroll and operate the YubiKey. The Help Desk was able to walk employees through a variety of different authentication flows to different applications and to allow for exceptions to any services that do not yet support WebAuthn. Once onboarded, employees have seen less friction in their authentication experience and better change management with self-service capabilities for lost keys or quick support for new devices.

Employees are encouraged to use their YubiKey to secure both their work life and their personal life. In fact, employees are free to take their YubiKey with them if they depart the organization, a commitment to helping employees see the value of using a YubiKey to protect themselves and to increase their comfort level with the workflow.

The future is passwordless

With organization-wide deployment of the YubiKey, the organization is already looking to the future of authentication—and that future is passwordless.

Passwordless authentication is any form of authentication that doesn’t require a user to provide a password at login. Combined with modern authentication approaches such as FIDO2, the organization can eliminate the username/password in its authentication flow to improve the user experience and offer the highest assurance security.

“A passwordless flow is a natural iteration,” says the Director of IT, “As we progress further and adopt new technologies, we want to move towards a passwordless future. Having YubiKeys already deployed helps us do that.”

Learn more | yubi.co/customers | yubi.co/technology

yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.