Solution Brief

Meet CISA Guidance With HYPR Passwordless MFA

Deploy phishing-resistant MFA that meets CISA guidelines and allows your workforce to securely access accounts and systems faster and easier

Introduction

On October 31, 2022, CISA (Cybersecurity and Infrastructure Security Agency) released guidance on threats against accounts and systems using certain multi-factor authentication (MFA) methods. The guidance strongly urges all organizations to implement phishing-resistant MFA, specifically FIDO-based authentication or, alternatively, PKI-based MFA such as the U.S. government's personal identity verification (PIV) or common access card (CAC).

Who This Guidance Affects

As the national cybersecurity agency, the CISA recommendations apply to all organizations in the U.S. The guidance advises phishing-resistant methods for all users and for all services. However, it recognizes some organizations may need a phased plan that begins with their critical resources and high-value targets.

Examples of Non-Compliant MFA Methods

Most organizations do not currently use phishing-resistant MFA. If your MFA is not fully FIDO Certified or a government-sanctioned PKI method, it does not meet the CISA guidelines for phishing resistance. This includes:

- SMS or voice
- Non-FIDO app-based authentication (one-time passwords, push notification token-based OTP)
- SSO-native authenticators — including MFA methods labeled passwordless
- IdP-native authenticators – including MFA methods labeled passwordless

Many solutions provide a passwordless user experience but they use a password on the backend or allow a fallback to a password or shared secret, so are not actually phishing-resistant.

HYPR Key Benefits

Uncompromising Security Assurance

- Meet CISA guidelines for phishing-resistant MFA
- Secure all access points, from desktop to cloud
- Stop phishing, fraud and account takeover
- Cover all your use cases including remote employees and shared workstations

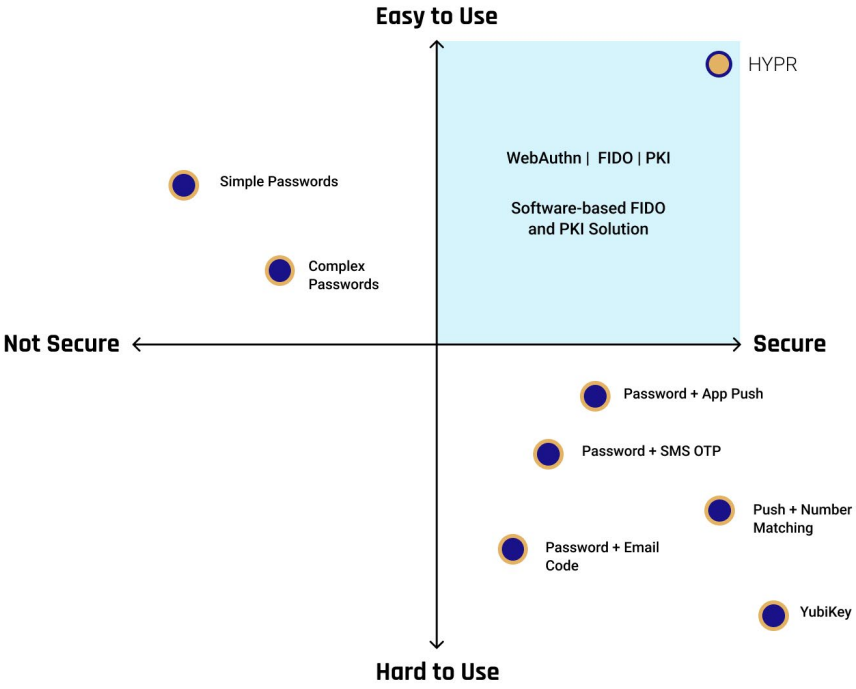
Consumer-Grade Experience

- Enable fast, easy login for employees and customers
- Eliminate password resets and improve productivity
- Integrate quickly with existing systems, IdPs and applications
- Onboard users in minutes

Why CISA Issued This Guidance

Cyber criminals continue to develop new attack techniques that target security weaknesses, especially in authentication. Conventional MFA cannot protect organizations in the current threat landscape. Attacks against Twilio, Uber, Okta, Dropbox and others succeeded despite these organizations having traditional MFA controls in place.

The CISA guidance maps various types of MFA to their threat susceptibility. Below is a visual representation of authentication security levels, combined with their ease of implementation and use.



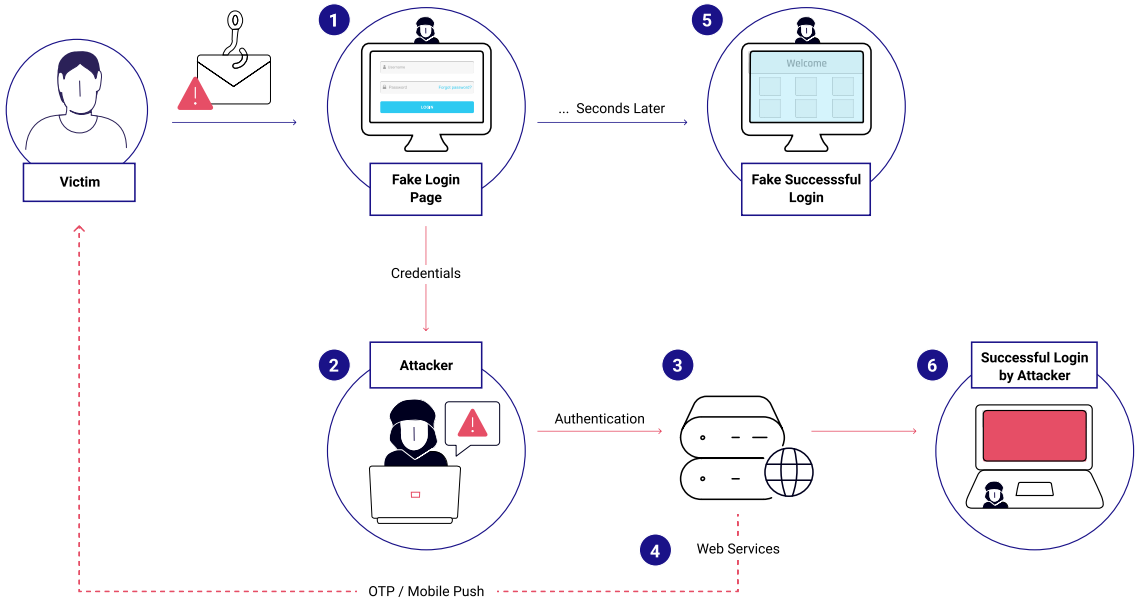
For the full CISA ranking of MFA forms and the specific threats they are vulnerable to, see "Table 1: MFA Forms, Strongest to Weakest" on page two of the Implementing MFA Fact Sheet published by CISA October 2022.

Cyberthreats Exploiting Authentication Weaknesses

Automated hacking tools use credential stuffing, phishing, smishing, MitM and other tactics in large-scale attacks that can defeat most legacy MFA methods.

A typical attack combines multiple techniques into a well-oiled, inexpensive to execute, attack flow.

Anatomy of an Attack



HYPR Provides CISA-Compliant MFA

HYPR True Passwordless™ MFA meets all CISA phishing-resistance specifications. As one of the first developers of FIDO-based passwordless authentication, HYPR's cutting-edge technology is purpose built to provide regulatory and guidance-adherent MFA that resists phishing while enabling frictionless access to digital resources and systems.

FIDO Certified End-to-End

HYPR is **the only solution** that is FIDO Certified across its entire product stack. Many solutions call themselves FIDO compliant but have not been certified by FIDO so their security levels and regulatory compliance status remains questionable. Others are FIDO Certified in a single component, such as the server. This means that to get FIDO-level phishing resistance, you need to use a separate FIDO Certified authenticator such as HYPR or a YubiKey.

Complete Desktop to Cloud Coverage

Organizations typically focus on securing logins to accounts and applications and neglect the risks posed by insecure desktop authentication. Employee desktops, workstations, laptops and consoles contain confidential data, browser-cached passwords, access to company communication apps and other resources that can be exploited by attackers. HYPR provides phishing-resistant, passwordless MFA that starts at desktop login and seamlessly carries through to downstream applications and services.This creates a "continuous authentication" security environment that is frictionless and invisible to the user.

No Vendor Lock-In

By using a fully FIDO Certified authentication solution, based on industry- and government-backed open standards, you expand your IAM interoperability and flexibility without being locked into a specific technology. Keep your current identity system or move to a new provider, deploy best of breed tools — your users will experience the same simple login flow across devices and channels.

Fast, Flexible and Field-Tested Deployment

HYPR is field-tested and deployed at scale in some of the largest and most complex environments globally, including two of the four largest US banks. HYPR installs rapidly and is fully integrated with leading single sign-on providers and IdPs. The HYPR PMFA platform supports multiple authenticator options including smartphone app, desktop platform authenticators such as Windows Hello and TouchID, and hardware security keys such as YubiKey.

MFA From the Passwordless Leader

There's a reason HYPR is called "The Passwordless Company™." Our phishing-resistant technology protects businesses large and small across the globe, with customers reporting up to 80% reduction in their attack surface.
By working with HYPR, you leverage a deep bench of authentication security expertise to expedite the development of your CISA-compliant MFA program. Contact a HYPR passwordless security expert to learn more.

THE PASSWORDLESS COMPANY

Email: info@hypr.com
Learn more: www.hypr.com

HYPR fixes the way the world logs in. HYPR's True Passwordless™ multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.