NEW-ERA AUTHENTICATION LENDS SUPPORT FOR FEDERAL ZERO TRUST INITIATIVE

The White House 'Executive Order on Improving the Nation's Cybersecurity' calls for accelerating attention on MFA solutions. What's new in authentication and why it matters.

FedScoop Report

As officials for Colonial Pipeline came to grips in early May with the latest, and possibly most public example yet of the cost of ransomware attacks, one aspect proved abundantly clear: Traditional perimeter security defenses are simply no match for determined hackers.

That's one reason why the White House's May 12 executive order, directing federal agencies to adopt zero-trust security principles, was greeted by many in the IT community as a welcome, if long-overdue shift for how organizations — and government agencies by example — need to rethink their secure strategies.

The executive order outlined multiple steps to modernize the government's cybersecurity systems, enhance software supply chain security, and remove barriers to sharing threat information. It also broke new ground by specifically directing agencies to develop plans to implement zero trust architectures — within 60 days of the order— and requires agencies to adopt multi-factor authentication and encryption for data at rest and in transit within 180 days.

The White House's call for a zero-trust strategy signals an important turning point in cybersecurity circles. It recognizes once and for all that relying on perimeter defenses alone to keep bad actors out is all but futile, given that adversaries are already inside our networks. That signal is also expected to reverberate beyond government data centers.

"This executive order will affect many organizations, both in the public and private sector, that work with the government [including] financial services, healthcare, the public sector, critical infrastructures, high tech, and education," commented David Treece, Director Solutions Architecture at Yubico, a global leader in secure access technology.

The concept of zero trust is hardly new to federal agencies. However, the sprawling nature of federal IT systems and pressure to comply with various FISMA, FedRAMP, CDM and other agency security requirements, have made it hard for federal CISOs to make much headway with a zero-trust agenda.

That's changing, thanks in part to the development of the National Institute of Standards and Technology's Zero Trust Architecture — the latest version of which was released in August 2020. There's also been added attention emanating from the Office of Management and Budget, with OMB M-19-17 and M-20-19 directives, giving agencies increasing guidance and flexibility to improve identity, credentialing and access management (ICAM).

Though still often mistaken as a technology in itself, zero trust at its core, represents a mindset as well as a collection of strategies to protect an organization's resources. It hinges, however, on creating a network environment where all individuals, devices and automated applications are authenticated continually and contextually; and where all are granted access to resources only on a least-privileged provisional basis.

That said, zero trust depends on having a modernized multi-factor authentication platform that can support today's widely distributed and dynamically configured networks, from the core to the edge, on-prem and in the cloud.

The limits of CAC/PIV cards

As has often been the case in technology, the federal government actually led the way in developing multi-factor authentication, dating back nearly two decades ago when the Department of Defense began rolling out its Common Access Card. Civilian agencies soon followed suit with Personal Identity Verification (PIV) cards.

Both had the advantage of providing users with two forms of authentication: something the user knows (their PIN) and something the user has (the card). An adversary would have to physically obtain the CAC or PIV card and also obtain the PIN to that card in order to gain access to a facility or an electronic system.

But the drawbacks of CAC and PIV cards became apparent almost immediately. Those working in command centers requiring simultaneous access to multiple systems discovered CACs limited their access to one system at a time. They also required specialized contact-based card readers — to prevent someone from eavesdropping on the traffic that goes between the card and the card reader — making them difficult to use with modern devices such as mobile smartphones and tablets.

Fortunately, in 2008, a small group of engineers from Yubico, recognizing the challenges, developed the YubiKey, a hardware security key that utilizes DoD-approved Public Key Infrastructure (PKI) cryptography and Identify Federation Service (IFS) solutions to authenticate users as an alternative to CACs.

Federal agencies have historically relied on PKI infrastructure to authenticate onto the network. So understanding that ICAM teams are focused on this environment, Yubico has worked with certificate authority (CA) vendors to open up support for PKI-based authenticators, by creating a Derived-PIV (or a PIV-D) workflow. That allows a certificate to be loaded on the YubiKey, ensuring that agencies can address their PKI authentication needs today, while the same YubiKey also gives them the flexibility to support emerging non-PKI authentication protocols when they are ready to do so in the future.

> **"YubiKeys provide a form factor that is as strong as the CAC or the PIV and can be used across multiple devices without a smart card reader.**
>
> ***– Jeff Frederick, Yubico***

"Government agencies can use the YubiKey to bridge the gap to the future", says Rob Konosky, Director for Yubico's federal defense business. "There's no reason to wait to start issuing hardware security keys such as the YubiKey to every single soldier, sailor, airman and marine that has strong authentication needs."

Modernized authenticators

Fast forward to the advent of cloud computing, users' ubiquitous reliance on multiple mobile computing devices, and most recently, the massive redistribution of the government's workforce during the pandemic. Collectively, it's never been more critical for agencies and enterprises to rely on modernized and adaptable alternatives to multi-factor authentication.

That's one of the reasons Yubico has been actively partnering behind the scenes with Google, Microsoft and other leading technology suppliers to advance the capabilities of remote authentication, says Frederick.

Most notably, Yubico is a founding member of the non-profit FIDO (Fast Identity Online) Alliance, formed to address the lack of interoperability among authentication devices. Yubico engineers have also teamed up with the Open ID Foundation, the World Wide Web Consortium and NSTIC — the National Strategy for Trusted Identities in Cyberspace. Behind those efforts is a mission to develop innovative, open, scalable and interoperable mechanisms which work effectively in the cloud and ultimately, are aimed at supplanting the reliance on passwords.

That's led to a comprehensive line up of YubiKeys that are trusted by the world's largest organizations. They allow users to access accounts four-times faster than other two-factor authentication (2FA) and cut support calls by 92%. And unlike other 2FA, YubiKeys store no data, require no network connection and don't run on software — which is why users have experienced zero account takeovers. And they work right out of the box with hundreds of enterprise applications.

Yubico's latest all-in-one multi-protocol YubiKey 5 FIPS Series is designed to meet the highest authenticator assurance level (AAL3) requirements from NIST for government and regulated industries.

"YubiKeys provide six, multi-factor authentication protocols all on one physical piece of hardware," says Frederick, including the ability to support both legacy and modern security protocols, using static passwords, one-time passwords (OTP), PIV (smart card), OpenPGP, FIDO U2F and FIDO2.

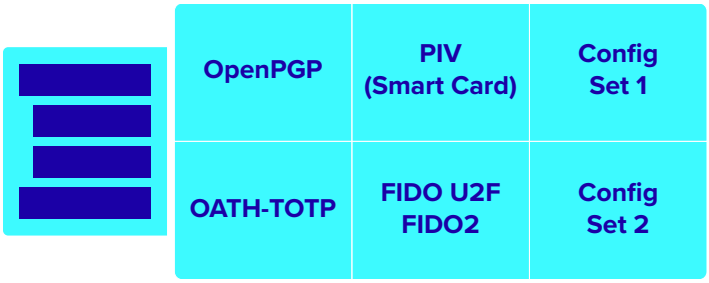
Additionally, Yubico designed the hardware so that the authentication secret is stored on a separate secure chip built into the YubiKey, so that it cannot be copied or stolen.

"That enables the highest-assurance, multi-factor authentication solution available across a wide range of legacy and modern clouds, applications, and devices," he says. "It's also the only FIPS 140-2 (Overall Level 2, Physical Security Level 3) certified multi-protocol token currently available; it's compliant with DOD's Cybersecurity Maturity Model Certification (CMMC) Level III requirements; and it is made in the USA, offering unparalleled supply chain integrity."

Enabling FIDO2 authentication

Yubico provides more than state-of-the-art USB and NFC (near-field communication) authenticators. It's also playing a larger role helping federal agencies develop stronger identity, authentication and encryption practices in working with the public.

> **SMS to your phone... is no longer enough. There have been too many hacks and vulnerabilities to that technology. FIDO is an easy-to-implement, easy-to-use solution for that.**
>
> ***– Fadi Jarrar, Yubico***



Multi-protocol security key secures modern and legacy systems.

Jarrar recommends that agencies consider implementing FIDO2 authentication protocols, especially in cases where citizens are encouraged to download information online, such as their annual Social Security benefits statement.

Agencies are still at different stages of recognizing the evolving nature of multi-factor authentication protocols. "Many agencies still don't understand the multi-protocol piece of this," he says. That's in part because "this industry in this area has changed exponentially. Some agencies are a little bit behind; some agencies are pretty forward thinking. But they all have a journey to go from where they are to essentially an end state revolving around FIDO."

Enable modern passwordless authentication with FIDO2

FIDO2 is the newest FIDO Alliance specification for authentication standards. WebAuthn is a web-based API that allows websites to add FIDO-based authentication on supported browsers and platforms. Together, they support an evolving security ecosystem that will make adopting modern passwordless authentication easier.

Your ability to implement a FIDO2 passwordless approach will depend on what you have in place already. If you are still operating in a Microsoft Active Directory (AD)-only environment with on-premises administration, then a smart card implementation is probably your best first step toward passwordless authentication. However, if you have cloud-based applications like Microsoft Microsoft Azure Active Directory (AAD) or a hybrid AD-AAD backend environment, then FIDO2 passwordless authentication is worth considering. If you are working with other identity providers such as Okta, DUO or Ping, you can also consider a FIDO2/WebAuthn based modern passwordless approach.

Jarrar notes that Yubico's participation in the evolution of MFA is one of the reasons "we are in discussions with just about every cabinet level agency," as well the Cybersecurity and Infrastructure Security Agency. CISA was testing Yubico's technology for different use cases ahead of the president's executive order; and Yubico played a part in supporting security in the Biden campaign and the president's transition teams, according to Jarrar.

"If [agencies] have already got something today, they can swap over to a FIDO2 authentication solution very quickly and easily," says Jarrar. "I think the new administration really does understand there needs to be a stronger way of authenticating citizen services across the board for the government."

Ultimately, adds Frederick, high-assurance authentication leads to greater user satisfaction as well as more trusted security.

Learn more about how Yubico can help accelerate your agency's journey to zero trust.

This report was produced by FedScoop and underwritten by Yubico.

FEDSCOOP yubico