Channel Partners™

A Guide to Improving Security by Eliminating Passwords

Passwords aren't going to disappear overnight, but implementing MFA solutions based on the new FIDO 2.0 standard promises to reduce credential theft. Now is the time to start planning your clients' password exit strategy.

By Jeffrey Schwartz

PRESENTED WITH

Channel Futures™

NOVEMBER 2018

TABLE OF CONTENTS

channelpartnersonline.com

S211118

ABOUT US

Channel Partners

For nearly 30 years, Channel Partners has been the leader in providing news and analysis to indirect sales channels serving the communications industry. It is the unrivaled resource for resellers, agents, VARs, systems integrators, cloud and digital services providers and consultants that provide network-based communications and computing services, applications, cloud services, managed and professional services — and more.

ChannelPartnersOnline.com is the official media partner of **Channel Partners Conference & Expo**, the world's largest channel event.

Channel Futures

Channel Futures unites the diverse ecosystem of companies that comprise the "evolving channel," which includes MSPs, systems integrators, born-in-the-cloud digital services companies, specialized services providers, agents, VARs and consultants who recommend digital services.

ChannelFutures.com co-produces the **CP Evolution** event.

Together **Channel Partners** and **Channel Futures** provide inspiration, insights and tools to help every partner thrive in a new, digitally transformed world.

About the Author

JEFFREY SCHWARTZ has covered the IT industry for nearly three decades, most recently as editor-in-chief of Redmond magazine and executive editor of Redmond Channel Partner. Prior to that, he held various editing and writing roles at Communications Week, Internet Week and VARBusiness (now CRN) magazines, among other publications. He is an editor-at-large for Channel Futures and Channel Partners.

linkedin.com/in/jeffschwartz
@jeffreyschwartz

A Guide to Improving Security by Eliminating Passwords

PASSWORDS ARE MORE THAN JUST an inconvenience these days; they're an outright liability. Besides the obvious frustration of help desk operators having to constantly reset forgotten passwords, misuse of passwords is costly as it is one of the most significant causes of security breaches.

The risks have only escalated in recent years as employees use their corporate credentials with mobile devices on public networks. But emerging solutions promise to eliminate passwords and simplify the implementation of multifactor authentication (MFA).

Organizations where employees must access sensitive or classified information often use smart cards and other specialized authentication tools to gain such access, but such tools are complex, costly and not suited for mainstream use. Many organizations also use hashed passwords. However, those carry the same risks as passwords.

Efforts to provide alternatives to passwords and deliver a horizontal approach to MFA have taken on more urgency in recent years, as stolen

Password Insecurity

The most common passwords found among two million to five million exposed annually in data breaches are predictable, making them easy for hackers to guess. The 10 most common, as collected by SplashData, a password-security software firm:

	2011	2012	2013	2014	2015	2016
1	password	password	123456	123456	123456	123456
2	123456	123456	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345
4	qwerty	abc123	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football
6	monkey	monkey	123456789	123456789	123456789	qwerty
7	1234567	letmein	1111	1234	football	1234567890
8	letmein	dragon	1234567	baseball	1234	1234567
9	trustno1	1111	iloveyou	dragon	1234567	princess
10	dragon	baseball	adobe123	football	baseball	1234

Source: SplashData

credentials have become the leading cause of successful phishing, ransomware attacks and breaches.

Everyday use of biometric authentication is still nascent, though it started to emerge as a viable alternative to passwords five years ago when smartphone and tablet providers began adding fingerprint authentication to their devices. And last year, iPhones and some Android devices began using facial recognition. However, those options don't eliminate passwords altogether.

Yubico's new YubiKey 5 Series USB-based passwordless keys boast FIDO 2.0 support.

Because people can't remember the myriad passwords they have – even if their organizations have a single sign-on or federated identity management solution – they default to risky behavior. Using easily guessed passwords or the same password across multiple sites is very common, as is writing them on Post-it Notes. These often facilitate data breaches; Verizon's Data Breach Investigations Report last year found that 81 percent of breaches are the result of stolen or weak passwords. Resetting passwords is also costly.

"One of the biggest problems with passwords is that … the end user … will never know when a password is used by a malicious user unless that malicious person wrecks something," said Sander Berkouwer, CTO of SCCT, a managed cloud service provider in the Netherlands.

Password replacement isn't going to shift from a novelty to an automatic capability overnight, but mobile solution providers need to get up to speed on what's available now and what will soon be available in terms of biometrics and MFA options.

In this report, we outline the latest developments in biometric authentication and MFA, as well as some of the problems with the way passwords are commonly implemented today.

FIDO Unleashed

Several years ago, Google wanted employees to stop relying on passwords for authentication into its network. The company rolled out YubiKeys from Yubico, which have embedded chips and can be connected to a device via USB, Bluetooth or near-field communications (NFC) to securely authenticate without a password. Microsoft employees, meanwhile, use Windows Hello for Business to log in and the company's Authenticator app for MFA. Both Google and Microsoft are using MFA based on the Fast Identity Online (FIDO) standard.

The two companies, which have been putting considerable emphasis on solving the password issue for many years, were among those that helped form the FIDO Alliance, a consortium that has grown to 270 technology providers and

business customers. FIDO's standards efforts have focused on creating a secure and interoperable approach to MFA and biometric authentication between hardware, software and commercial websites.

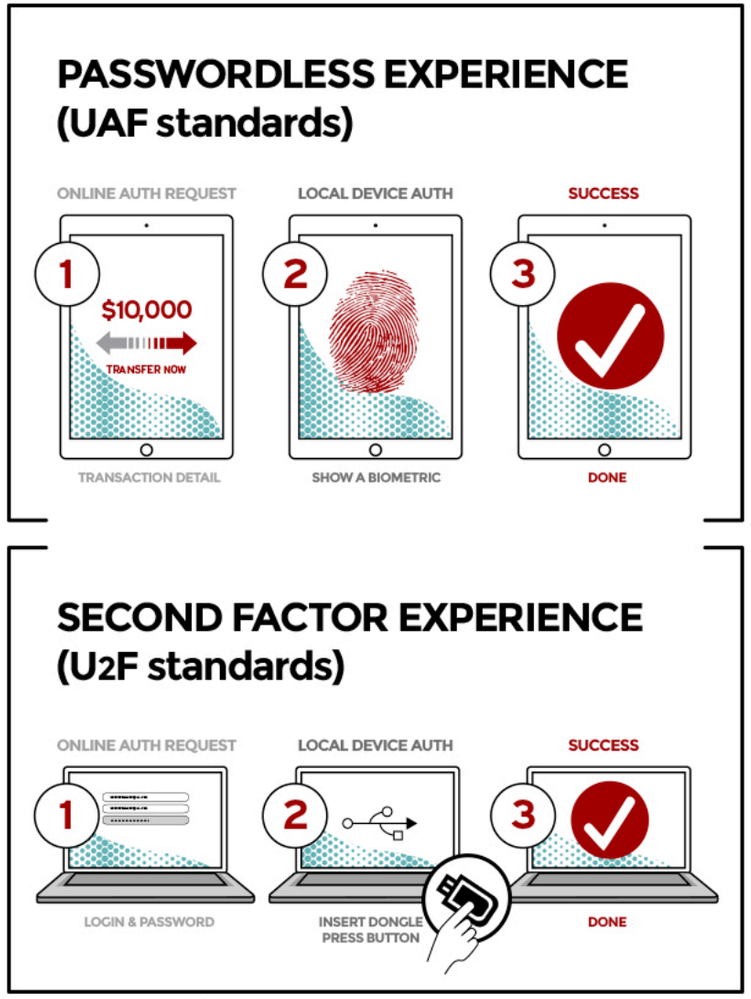
Nearly four years ago, the consortium published the FIDO 1.0 specifications. The specs, which include the Universal Authentication Framework (UAF), allow a user to register a device, application or website, and use supported authentication methods such as a PIN, a fingerprint or a facial image. After the authenticators are registered to the device, the user can authenticate with the modes registered with UAF. FIDO 1.0 also includes Universal Second Factor (U2F), which users can present with USB-based keys from companies such as HID and Yubico.

Microsoft built Windows Hello with FIDO support. Windows Hello is the biometric authentication capability introduced with Windows 10 that logs users onto PCs that have compatible fingerprint readers or facial recognition sensors. Microsoft recommends PCs with Trusted Platform Modules (TPM) when using Windows Hello.

This year, the consortium ratified the FIDO 2.0 standard, which adds stronger web authentication. FIDO 2.0 is built around the new, advanced Web Authentication (WebAuthn) protocol that allows secure access from Google Chrome, Microsoft Edge and Mozilla Firefox to supported websites.

FIDO 2.0 also includes the Client to Authenticator Protocol (CTAP), which allows a mobile phone or security key to create links using strong encryption protocols via USB, Bluetooth or near-field communications (NFC) to the client device. For example, Yubico's new YubiKey 5 Series supports FIDO 2.0's WebAuthn, FIDO U2F, PIV (smart card), OpenPGP, Yubico One-Time Password (OTP) and challenge-response, among others.

The FIDO Alliance claims its specs will work on 80 percent of the mobile devices now available and there are now more than 400 certified products. In September, the alliance announced the Biometric Competent Certification Program to validate claims.



Source: NetworkWorld.com

Now Google has its own key, the Titan Security Key, which is a USB key that supports Bluetooth and NFC. Google also recently launched MFA access to G Suite and Google Cloud with the new key. Customers and service providers can implement a control that requires usage of the key from the admin console.

At Microsoft's annual Ignite conference for IT professionals, held recently in Orlando, Fla., company officials gave significant airplay to new capabilities in the most recent fall update of Windows 10, Azure Active Directory and related offerings that will help make biometrics and MFA in the workplace a reality. "This multifactor authentication, or 'passwordless' future, has to be done in a way that user adoption is at the center of it," Microsoft CEO Satya Nadella said at Ignite.

Microsoft is promising this is a near-term deliverable, not a future vision. "We're at the point now where I feel really confident that we can declare the beginning to the end of the era of passwords," said Alex Simons, vice president of program management within Microsoft's identity technology group. "Within 120 days or so, there will be no reason why you should need to use a password with any Microsoft-connected application ever again."

Google's two-step verification access allows users to authenticate to their Google account with a FIDO 2.0 security key such as YubiKey and Google's own new Titan.

The quest to eliminate passwords is not a new one for Microsoft, which has touted the idea since gearing up for the launch of Windows 10 three years ago. At the time, Windows Hello only worked on Microsoft's Surface line of PCs and a handful of commercial PCs from OEM partners and third-party peripherals such as YubiKeys.

In September, Microsoft claimed that 69 million users authenticate with Windows Hello, up from 37 million a year ago. For commercial and enterprise users, Microsoft added Windows Hello for Business, a version that makes use of Active Directory, Azure Active Directory Premium controls such as Group Policies and mobile device management (MDM) settings and supports certificate-based authentication.

Microsoft reports that 6,500 enterprise customers are using Windows Hello for Business, an increase from just 300 organizations last year. In Windows 10 version 1803, released in April, Microsoft added support for third-party management and certificate enrollment APIs and WiFi as a trusted signal in multifactor unlock to Windows Hello for Business. The latter is a feature that allows proximity to a signal such as a paired phone via Bluetooth as a factor in Windows Hello when using MFA.

The newest October 2018 release, Windows 10 1809, allows Remote Desktop using biometric authentication and Azure AD Join without passwords.

Microsoft Authenticator App Joins Azure AD

The death of the password may not come as imminently as some of the latest developments may suggest, though you can expect to see many more organizations shifting in that direction in the coming year. Microsoft's journey to eliminating passwords took a key step last year when the company updated its Authenticator app with support for Windows Hello for Business. The

Authenticator app delivers MFA, allowing users to log in to Windows and other Microsoft services and applications.

Microsoft's newest update to Authenticator replaces the password by implementing MFA to sign in to multiple apps by combining a fingerprint, facial recognition or a PIN. It can be set up so that users will only stay logged on if their phone is nearby (via Bluetooth or NFC connection). MFA can reduce the risk of a password compromise by 99.9 percent, according to Microsoft. The latest release of Microsoft Authenticator supports integration with Azure Active Directory.

"No company lets enterprises eliminate more passwords than Microsoft," said Corporate Vice President for Security Rob Lefferts.

SCCT's Berkouwer, a Microsoft MVP specializing in directory services, noted the improvements to Authenticator. "I guess you can only show this level of innovation when the codebase of an app is of good quality," he said. "It has taken Microsoft some time to get there, but they're now delivering at breakneck speed."

The Problem With MFA

Even with the 99.9 percent reduced risk of compromise, Berkouwer suggested that because Microsoft has 17.5 million Azure AD tenants today, statistically a compromise happens to every 100,000 tenants. "It happens quite often," he said during a session at Ignite. "MFA fishing is turning into a big problem."

"Passwords are bad and multifactor authentication isn't the answer, but [it is] the best thing we have."

—Sander Berkouwer, CTO of SCCT

When people use SMS-based texting as a factor in MFA, while it might be better than just using a password, it comes with risks, he warned. Organizations implementing MFA should upgrade to something stronger. "Passwords are bad and multifactor authentication isn't the answer, but [it is] the best thing we have," he said.

Microsoft is advising partners and customers to start deprecating virtual smart cards on Windows 10 and deploying Windows Hello for Business. In early 2019, the company will release the technical preview of Windows Hello Security Keys that support FIDO 2, allowing for authentication into non-shared devices and those that are Hybrid Azure Active Directory-joined. The latter scenario applies to those that are both Active Directory-joined and connected to Azure AD. The Windows Hello Security Keys will also provide access to on-premises resources and Remote Desktop.

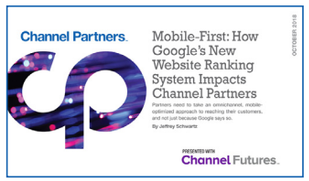
At the very least, Berkouwer said he encourages organizations to upgrade to Windows 10 and use Windows Hello for Business while keeping an eye out for an update with FIDO 2 support, which is currently in private preview.

Until your clients' customers are ready to get rid of passwords, Berkouwer suggests reminding them of the basics. "If you rely on passwords, only have people change them when they've been compromised or if their accounts run another risk of getting taken over," he said. "In some organizations, eradicate reuse of the same passwords."

Related Reports

Giving MSPs an Edge: A Guide to Building a Comprehensive Security Portfolio

With the volume of cyberthreats on the rise, organizations are scrambling to stay one step ahead of cybercriminals. This spells big opportunities for MSPs and MSSPs. But to get an edge on the competition, you need to pick the right security tools. In this report, you'll learn which managed security services to offer.



Mobile-First: What Google's Change to Ranking Websites Means to Channel Partners

Earlier this year, Google changed the way it indexes websites. Those sites not optimized for mobile devices will be penalized significantly in search engine rankings. But that's not the only reason partners need to take an omnichannel, mobile-optimized approach to reaching their customers.

7 Channel-Changing Mobility Trends for 2018

We're seeing a new wave of innovation in mobile technology and market focus. Going forward, enterprises and their trusted advisers need to stay abreast of how mobile operators are supporting IoT, 5G, VoLTE and other emerging techs — some of these initiatives will have major implications for enterprise networks.