E-BOOK

Got Phished?
How to Get MFA Right the First Time

SECRET
DOUBLE
OCTOPUS

Contents

Introduction:

We’re Heading for Phishing-resistant MFA — and How You Get There Matters

Logging in used to be simple. Too simple. So, IT leaders raced to add a second, third, or even fourth step to the authentication process to strengthen security and meet evolving mandates for MFA.

And now it’s too complicated. Users hate the extra added steps, IT still gets bombarded with password-related calls, and worst of all, what we’re doing now hasn’t stopped the phishing that leads to ransomware and other nasty attacks.

Is it time to pivot?

The question is: Should you, as an IT leader, keep going down a path that effectively just reinforces passwords or pivot to a phishing-resistant passwordless MFA now — or keep investing in solutions that will aggravate users and never be enough?

Phishing-led attacks continued to grow at a rate of more than 60% in 2022[1]. Combined pressure from ransomware attacks, new government mandates, and rising cyber insurance premiums makes phishing-resistance a growing priority all around.

Can MFA ever stop phishing?

On the surface, the answer seems to be no. Passwords are easy to exploit and attackers continue to innovate new tactics, techniques, and procedures (TTP) to get around MFA as we know it today.

The traditional approach to MFA needs to change — before companies invest and get too far down the road. This paper will expose the fundamental flaw in today's MFA and how you can make sure your approach delivers on what should be its foundational promise: Make the user resistant to being exploited.

The change in question? To remove our dependence on proving user identity through passwords and removing tricky decisions — "should I click this link or OK this request I keep getting from IT" — without driving users or IT crazy.

Only 26%

of companies use MFA in the US

DataProt

$40B

MFA market 2030

Allied Market Research

21% CAGR

MFA market projected growth 2023-2027

Technavio

3B

phishing emails sent per day accounting for about 1% of all email

IBM

90%

of successful cyber-attacks start with a phish

Shields Up 2022

255M

phishing attacks occurred in 6 mos. in 2022

Slashnext

61% increase

phishing emails vs. 2021

Slashnext

$4.91B

average cost of a data breach with phishing as initial attack vector

IBM

295 days

breaches caused by phishing had the third highest mean time to identify and contain

IBM

Why MFA can’t wait

When the workforce went home back in 2020, IT teams worldwide stepped up and accelerated business digitalization virtually overnight. This accelerated modernization created an “all-hands-on-deck” situation that paved the way for opportunists to launch devastating ransomware and supply chain attacks against enterprises.

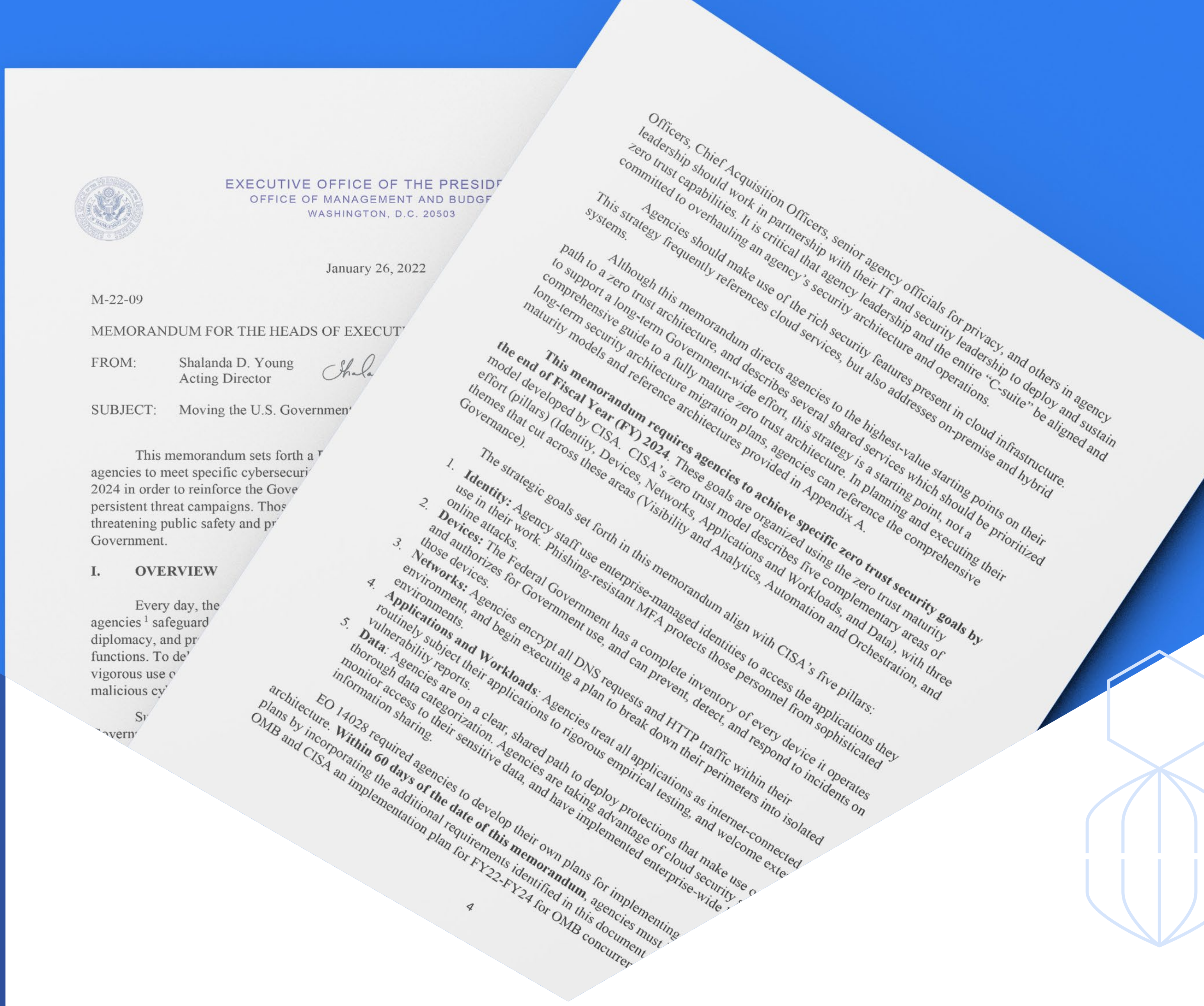
Nearly all attacks begin by exploiting users and very often use phishing, attackers’ favorite evergreen threat vector, to steal credentials, trick users into facilitating entry, and ultimately exfiltrate data or demand ransoms.

Regulators are turning up the heat

Businesses worldwide now face federal and industry mandates that push toward Zero Trust security postures and phishing-resistant MFA:

- Edicts such as memorandum 22-09, from the Biden administration’s Office of Management & Budget (OMB), mandate phishing-resistant MFA for the government supply chain by 2024
- De facto cybersecurity frameworks like MITRE ATT&CK stress phishing-resistance
- Cyber insurance discounts for demonstrating phishing-resistance won’t lag far behind

Nobody likes deadlines, but there’s no arguing the logic. Stolen or compromised credentials remained the number one cause of breaches in 2022[2] and attacks beginning with phishing as the initial threat vector cost companies $4.91M on average, significantly higher than the overall average cost of $4.35M.



EXECUTIVE OFFICE OF THE PRESID
OFFICE OF MANAGEMENT AND BUDG
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUT

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Governmen

This memorandum sets forth a
agencies to meet specific cybersecuri
2024 in order to reinforce the Gove
persistent threat campaigns. Thos
threatening public safety and pr
Government.

I. OVERVIEW

Every day, the
agencies [1] safeguard
diplomacy, and pr
functions. To de
vigorous use o
malicious cy

S
overn

Officers, Chief Acquisition Officers, senior agency officials for privacy, and others in agency leadership should work in partnership with their IT and security leadership to deploy and sustain zero trust capabilities. It is critical that agency leadership and the entire “C-suite” be aligned and committed to overhauling an agency’s security architecture and operations.

Agencies should make use of the rich security features present in cloud infrastructure. This strategy frequently references cloud services, but also addresses on-premise and hybrid systems.

Although this memorandum directs agencies to the highest-value starting points on their path to a zero trust architecture, and describes several shared services which should be prioritized to support a long-term Government-wide effort, this strategy is a starting point, not a comprehensive guide to a fully mature zero trust architecture. In planning and executing their long-term security architecture migration plans, agencies can reference the comprehensive maturity models and reference architectures provided in Appendix A.

This memorandum requires agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024. These goals are organized using the zero trust maturity model developed by CISA. CISA’s zero trust model describes five complementary areas of effort (pillars) (Identity, Devices, Networks, Applications and Workloads, and Data), with three themes that cut across these areas (Visibility and Analytics, Automation and Orchestration, and Governance).

The strategic goals set forth in this memorandum align with CISA’s five pillars:

1. **Identity:** Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
2. **Devices:** The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
3. **Networks:** Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.
4. **Applications and Workloads**: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome exte vulnerability reports.
5. **Data**: Agencies are on a clear, shared path to deploy protections that make use o thorough data categorization. Agencies are taking advantage of cloud security monitor access to their sensitive data, and have implemented enterprise-wide information sharing.

EO 14028 required agencies to develop their own plans for implementing architecture. **Within 60 days of the date of this memorandum**, agencies must plans by incorporating the additional requirements identified in this document OMB and CISA an implementation plan for FY22-FY24 for OMB concurre

4

The U.S. OMB memorandum 22-09 reads:

- MFA must be enforced at the application layer instead of the network layer
- For agency staff, contractors, and partners, phishing-resistant MFA is required
- **For public users, phishing-resistant MFA must be an option**

Why the focus on passwords

User frustration with the MFA companies have been rolling out is off the charts[3]. Getting rid of passwords represents less risk — with less steps — with greater convenience and greater productivity. What's more, mobile smartphone ubiquity and inexpensive FIDO2 tokens make eliminating passwords viable today. Why keep doing what we know doesn't work just because we've been doing it since the 1960s?

In this book, we'll show how you can build phishing-resistant MFA right now at lower cost and with infinitely less hassle than you might think. We'll cover:

- The growing focus on MFA
- How the bad guys are stepping up their game with man-in-the-middle (MITM) attacks
- Why traditional MFA doesn't stop phishing
- How to become phishing-resistant right now — without starting over
- How to keep IT in control at all times!

Chapter 1:

MFA vs. Phishing-resistant MFA

Phishing has been around since the ‘90s so it’s tempting to conclude that it might never get fixed. Now that it has to, the authentication process represents the obvious point to intercede and stop users from relinquishing the keys to the kingdom.

Companies invest heavily in spam filtering, and user education — all of which helps — but the bad guys “just need one” username/password combo to gain access and start targeting crown-jewel assets.

“What users know” is phishable

Passwords, PINs, and answers to security questions all represent “things users know” that can be leveraged to access websites, SSO portals, business accounts, and privileged databases. Some hackers buy credentials on the dark web, but phishing for active, working logins in real time is still cheap and easy.

47%

phishing emails successful

Duo

5%

Internet users fooled by phishing emails

Duo

MFA creates friction. . .

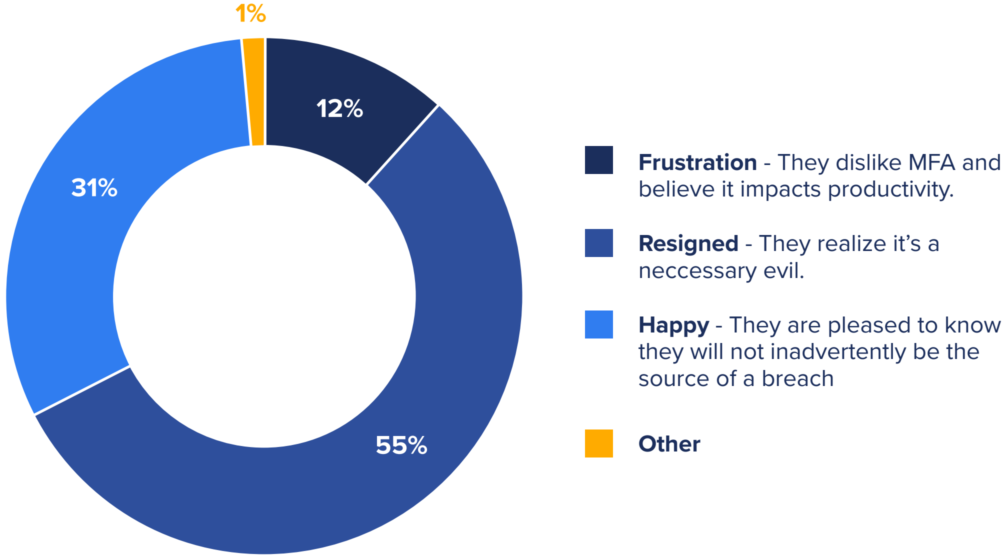
Where two-factor authentication (2FA) mostly just asked users to do one more simple thing to prove their identity — usually typing in a 4- or 6-digit one-time passcodes (OTPs) sent via text — today's MFA layers more annoying steps into the log-in process. Physical USB-type security keys, smart cards with X.509 certificates, facial scanners, thumbprint readers, and voice recognition now all may be part of the process.

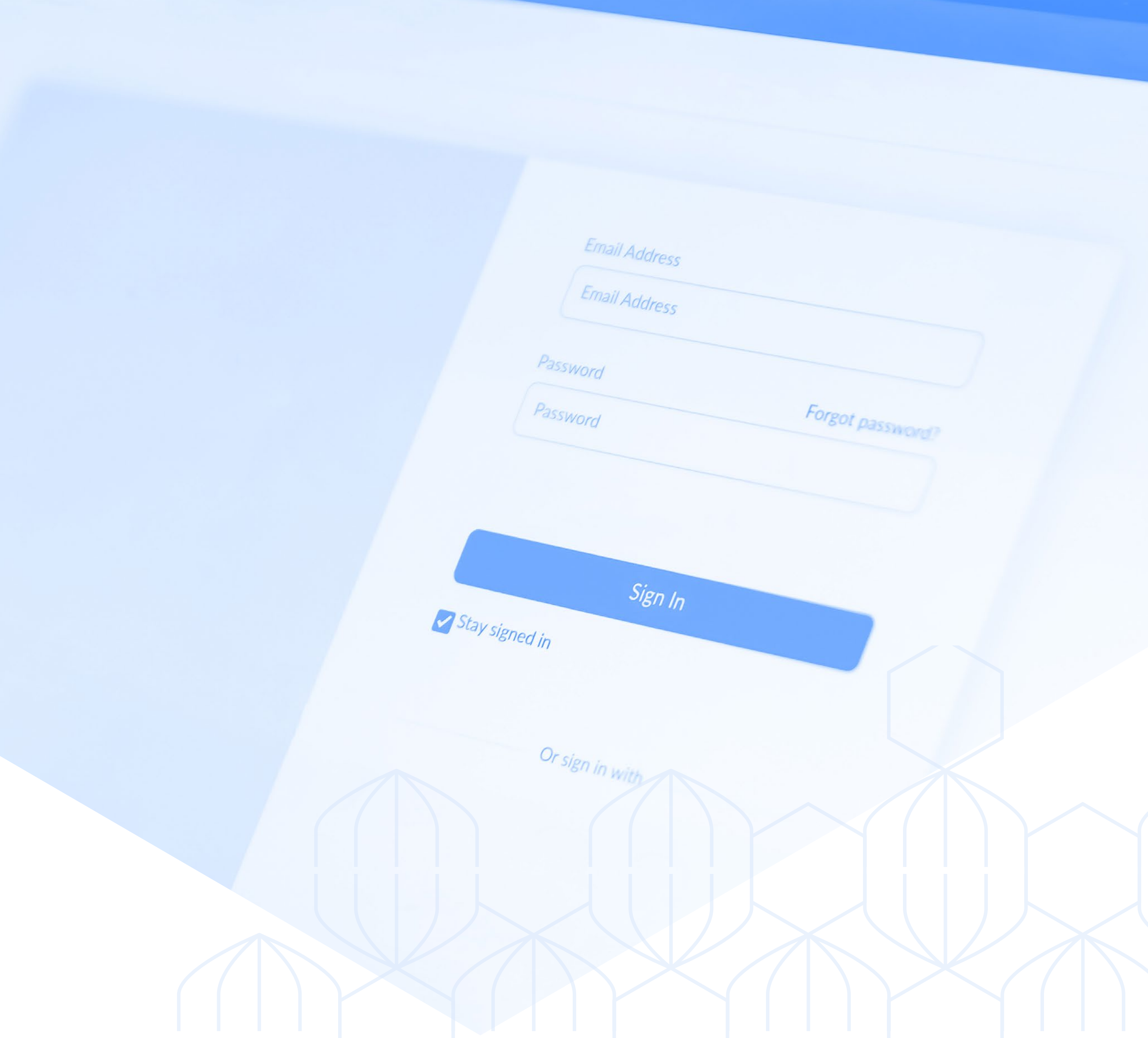
And the more complicated we make it to log in, the more users (and IT) hate MFA:

- **Users spend up to 5% of their time,** about 22 minutes a day, just authenticating[4]
- **Costs go up as IT buys,** ships, and maintains smart cards, hardware tokens, and biometrics readers across an enterprise workforce
- **Up to 50% of Help Desk calls** still involve credentials — to the tune of over $1 million per year in lost productivity

"To the best of your knowledge, which of the following best describes the attitude of a typical employee of your organization towards MFA?"

Dimensional Research





The good news, and reason to continue, is that, along with "something users know," today's MFA adds stronger pillars of identity verification. One is "something users have," typically their phone or PC, and also something they "are," verifiable with biometrics.

The bad news is: we're still getting phished.

The phishing problem is yet to be solved

MFA as we know it doesn't stop phishing because it continues to use credentials — the highly vulnerable "something users know"— as factor #1 in verifying identity. This foundational flaw keeps MFA intrinsically vulnerable to phishing, and in turn ransomware, malware, and third-party attacks that often involve innovative, targeted techniques and "man in the middle" attacks (we'll dive deeper into these in Chapter 4).

Where do we go from here?

Conventional wisdom is circling around to the real problem: traditional MFA still uses passwords. And to the *real* real problem, that these should-be secrets are still managed by users instead of IT. With its continued reliance on what users know, traditional MFA as we know it:

- Causes friction
- Adds cost
- Wastes time
- Fails to make us phishing-resistant

Piling on more steps will never be enough to check the box on phishing-resistance. One obvious way to bridge the remaining gap is to eliminate the use of passwords from the user authentication equation.

> "Despite spending an average of $73 on annual license fees and maintenance per user, respondents estimate that an average of 41 percent of attacks are targeting passwords and traditional MFA methods."
>
> Ponemon

Spending more on the same things won't solve the problem.

23.4M

phishing security tests

KnowBe4

9.5M

users

KnowBe4

30.1K

organizations

KnowBe4

5% **after one year of training clicked the bait.** KnowBe4

Chapter 2:

Taking Passwords Out of the Equation

Why drop passwords as you add MFA?

The goal of authentication — verifying the identity of someone trying to access certain resources — does not intrinsically need to include passwords, but it more or less always has. So, how do we remove the risk inherent in credential-centric login — phishing that plays a role in 80% of breaches — **without starting from scratch?**

Passwordless MFA is MFA that takes the perennially vulnerable "what users know" out of the equation. This immediately translates into business savings of nearly $2M achieved by:

- Streamlining the login process
- Transferring management of secrets to identity teams
- Eliminating MFA fatigue on both sides
- No longer feeding the phish **— finally!**

Passwordless MFA improves user experience (UX) and gives IT more time, flexibility, and budget available to modernize your identity and overall IT infrastructure — while eliminating versus exposing you to risk.
So, how do we do it?

What constitutes phishing-resistant MFA?

The term phishing-resistant MFA first appeared in the M22-09 presidential memo mentioned above, which didn't spell out exactly what was required. Implicitly, the requirements for phishing-resistant MFA are that it be:

- Impersonation-resistant
- Replay-resistant
- MiTM-resistant

The Cybersecurity & Infrastructure Security Agency (CISA) implementation guide lists two options for implementing phishing-resistant MFA:

- Public key infrastructure (PKI)-based government-issued PIV and CAC ID smartcards
- FIDO/WebAuthn authentication

CISA also recognizes that neither approach can go the distance in addressing all workforce applications. Even in "cloud-first" organizations, some percentage of applications use directories that will require passwords for a decade or two. In the meantime, CISA, NIST, MITRE ATT&CK, and other mandates and security frameworks prescribe phishing-resistant MFA.

PKI PIV and CAC ID smartcards

PKI uses a pair of public and private keys for authentication. Most PKI implementations exist within government agencies or other heavily regulated industries where workers carry smart cards with embedded X.509 tokens. These cards are expensive to deploy and rigid to maintain, so adoption has been low for broader enterprise use cases.

Newer software-based implementations like Windows Hello for Business or other X.509 certificate-based authentication systems use internally signed certificate-issuing infrastructure without physical smartcards. PKI also requires significant retooling of both applications and directory infrastructures to get full use case coverage (read: IT will be burdened for an unspecified length of time).

Systems may be incompatible with common use cases like Radius VPN, Linux-based services, and mission-critical custom and legacy apps that are dependent on password directories and PKI unsupported protocols.

FIDO works well for web

CISA calls FIDO, “the only widely available phishing-resistant authentication” but it’s only “widely available” for web or browser-based services. Developed by the FIDO Alliance and published by the World Wide Web Consortium (W3C), the WebAuthn protocol specified within the FIDO2 standard found rapid traction among leading browsers.

For greenfield web-only unicorn companies, FIDO2 WebAtuhn amplified by SAML may work, but for most businesses, the hub centers around password directories. To date, the FIDO Alliance has yet to release a standard for how FIDO2 tokens communicate with corporate apps that work with directories. A bridging function, like the Octopus platform described below, translates the FIDO2 token registered in the FIDO2 server to password directories and ultimately to corporate apps.

> “Successfully deploying PKI-based MFA requires highly mature identity management practices. It is also not as widely supported by commonly used services and infrastructure, especially in the absence of SSO technologies.”
>
> CISA

Passwordless MFA delivers the rare ROI trifecta:
Less risk, less cost, less complaints.
But can we do it today?

82% of breaches; stolen credentials phishing, misuse, human error

22 minutes /day Average worker time lost daily interacting with IT

BBC

8x productivity ROI Pays business diavidends **35x security risk buy down ROI**

The foundational step is passwordless

Strong authentication will ultimately be passwordless for one simple reason: eliminating user-managed credentials takes the phish out of the sea. Users can't share what they don't know exists.

Passwordless user MFA satisfies the intent of Zero Trust and phishing-resistant mandates — and will soon be a bonus for cyber insurance premiums — because it actually stops phishing (and the breaches that follow). All that needs to happen to achieve phishing-resistance is the transfer of password management to IT to take the secrets out of users' hands.

Pre-pinning adds the missing "link"

PKI and FIDO2 use public/private key pairs to establish trust. Users pre-register their FIDO2 devices with specific web sites or SSO portals. This approach resists phishing, including today's advanced MITM attacks because, no matter what information users inadvertently let slip, including the public key used in authentication, the hacker's device won't have the private key needed to decode the signing public key and verify identity. The private key never leaves the FIDO2 vault within the FIDO key or token.

The same approach can be implemented without hardware-based FIDO tokens or physical keys.

To expand the use of pinning — and passwordless MFA — beyond web applications, Secret Double Octopus (SDO) created desktop-to-application pinning. A software-based Octopus passwordless agent installed on user devices lets devices be directly pinned to individual SSO portals and other workforce resources without additional hardware.

The SDO agent prompts the trusted platform module (TPM) already inside the user's computer to generate a private key. The platform binds the private key with the public key to conduct secure identity verification via keypairs all within software.

It pays to do MFA right

As we have seen in recent years with some public cloud deployments, going down the wrong road carries significant cost, risk, and unwanted friction. This same thing is happening in MFA as companies invest heavily in devices, apps, onboarding, education, and support without accomplishing the main goal of reducing the business's attack surface.

While vendors define passwordless MFA differently, SDO believes it needs to satisfy four important goals:

- Less risk
- Less friction
- Less change
- Less cost

For this, we prescribe choosing a solution that meets five key criteria — right now — so you don't have to do it all again.

Chapter 3:

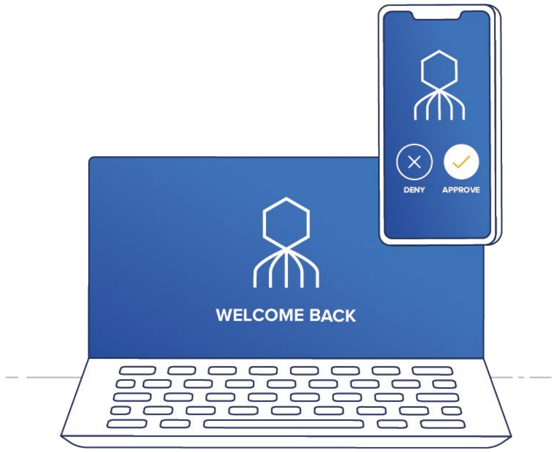
The Five Key Elements of Phishing-resistant Passwordless MFA

1. Users don’t need to set or change their passwords — ever

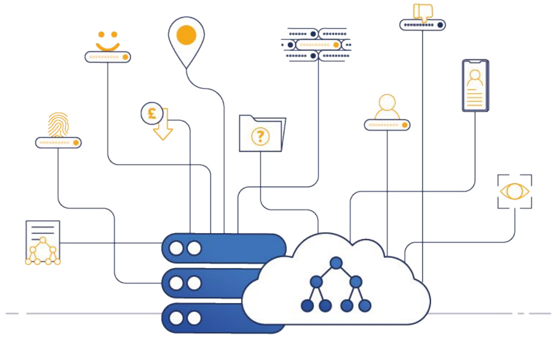
The key word here is “never.” The vast majority of solutions claiming to be passwordless actually mean “passwords-less-often.” Single sign-on (SSO) streamlines access significantly but isn’t passwordless, or phishing-resistant. Users still have to enter credentials upon startup, or “just once a day.” The password threat continues to exist.

2. User MFA gets decoupled from directories

A picture is worth 1,000 words:



Passwordless MFA



Password Directories

With directories remaining password-centric for the foreseeable future, coexisting with passwords on the back end is a must. Decoupling the back and front ends lets users be passwordless everywhere, right now while the majority of non-Web business applications continue to use passwords to authenticate into directories. Decoupling makes it easy to transfer password management and rotation away from users to the unphishable, behind-the-scenes realm of IT. And, ***IT can start onboarding users in less than hour.***

This “password directory-friendly” approach lets IT automate password rotation as often as they like — even daily — with no extra effort. Users don’t even know it’s happening. Directories don’t need to be retooled or upgraded until IT feels ready.

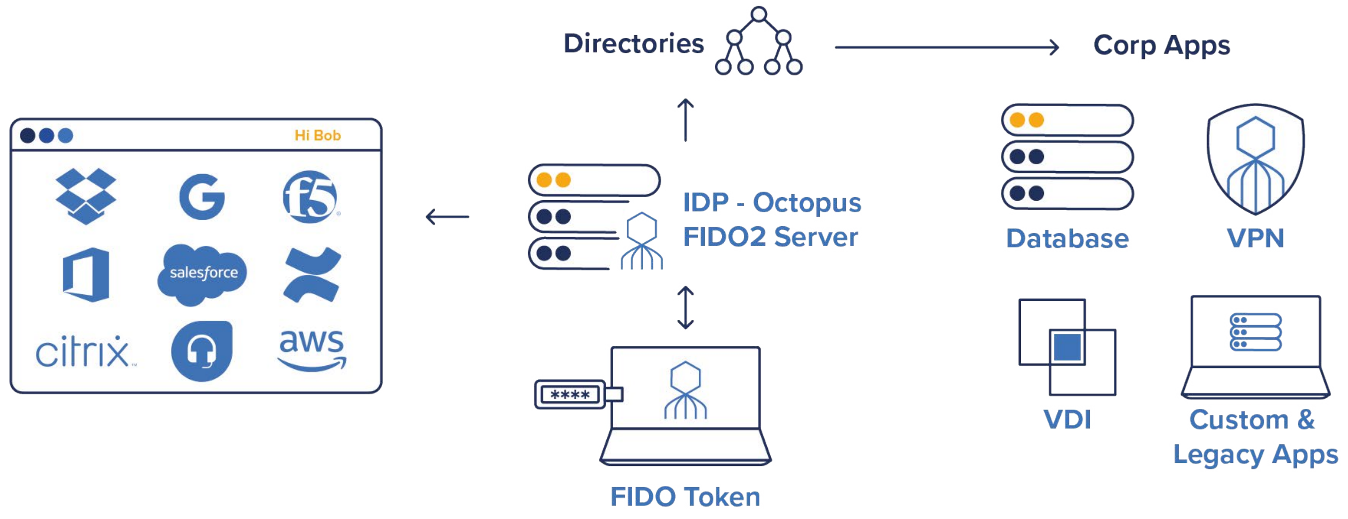
The de-coupling of user-side MFA from directories enables our third criteria.

3. All applications become phishing-resistant

Otherwise, you aren’t phishing-resistant. Sophisticated attackers do their homework to find the weak links in the chain. This might include older legacy or corporate applications, remotely accessed facilities in industrial environments, or users working from home who share their Wi-Fi — and the passwords that unlock their home PCs — with those around them.

Combining biometrics with pre-pinning makes it virtually impossible for anyone else to access devices and privileged applications and databases. Users get what they need to maximize productivity: A single workflow for desktop, corporate apps, privileged access, and web apps.

The Octopus supports FIDO2 WebAuthn through its certified FIDO2 server and can translate FIDO2 to corporate apps



Directories

Corp Apps

Hi Bob

IDP - Octopus FIDO2 Server

FIDO Token

Database

VPN

VDI

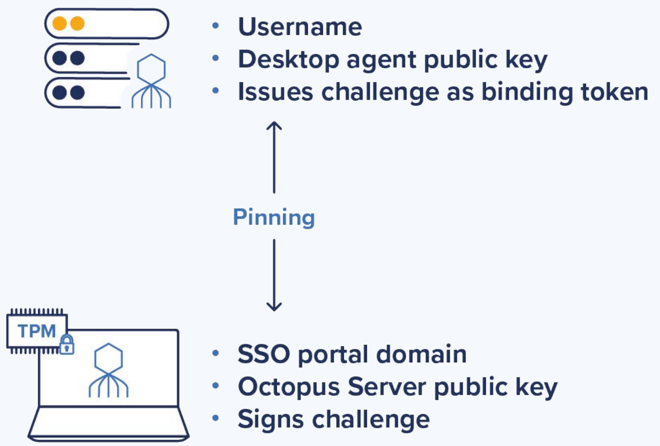
Custom & Legacy Apps

4. Works with mobile push

While many users are able to buy and provision FIDO keys on their own, most vastly prefer the simplicity of push notifications, and so does IT. There’s nothing to buy, nothing to carry, and best of all, nothing to lose.

Users love mobile push because it’s fast and easy and doesn’t require external devices (though biometrics like fingerprint readers can still be used for a second or third factor of verification).

Desktop-to-app pinning



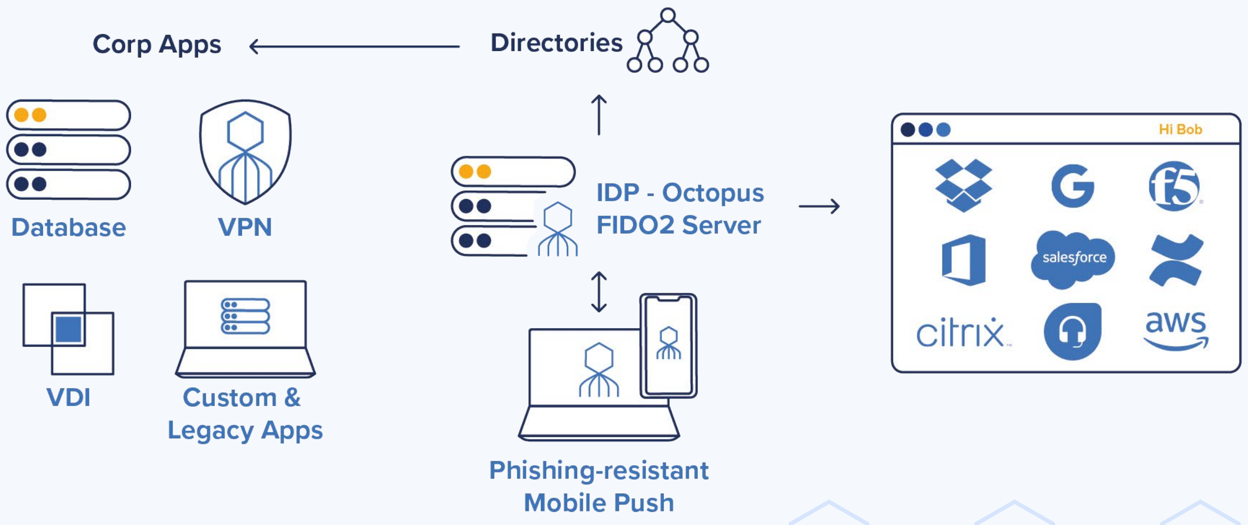
- Username
- Desktop agent public key
- Issues challenge as binding token

Pinning

TPM

- SSO portal domain
- Octopus Server public key
- Signs challenge

Desktop-to-app pinning integration



Corp Apps

Directories

Database

VPN

VDI

Custom & Legacy Apps

IDP - Octopus FIDO2 Server

Phishing-resistant Mobile Push

Hi Bob

5. Stops modern attacks

This is a huge topic, worthy of its own short chapter.

Chapter 4:

Four Ways Passwordless MFA Stops Modern Phishing Attacks

1. Phishing for credentials

Pretty straightforward: Passwordless MFA stops phishing campaigns aimed at tricking users into giving up their credentials because, so far as users are concerned, credentials don't exist.

2. Attacks on traditional MFA

Phishing-resistant MFA shields the workforce from techniques such as push bombing that target MFA itself. As we've seen with highly publicized recent attacks, users will give in when flooded with too many push notifications and/or fake messages from IT to approve the requests — even at 3 AM when they aren't logging into anything.

Pinning makes it impossible for hackers to start unauthorized authentication. They can't, because they won't have the right private key tucked away in the TPM vault or the right fingerprint/retina needed to finish the challenge.

3. Attacks on desktop and corporate applications

As described here, phishing-resistant MFA needs to extend beyond web apps that use WebAuthn to include all enterprise workforce use cases. Most companies rely heavily on the likes of VPNs, thick client apps, and devices that use Mac or Linux OSs. Password directory-friendly passwordless MFA with direct pinning makes it possible to include any device or application.

4. MITM attacks

The ultimate proof that we need to take people out of the process is that automated MITM attacks succeed with devastating silence once the bait is clicked, without exploiting passwords or second OTP factors. Attackers sit between a real target site and dynamically create an exact replica.

Modern attacks use automation, sending messages that trick users into attempting to authenticate into fraudulent locations to capture session tokens. With the token, the attacker has full access to the victim's account to modify credentials for account takeover or pivot off the victim toward more valuable company assets.

The only way to stop these attacks is for the user to spot the fake URL, which is especially unlikely with long URLs. Or you can apply phishing-resistant MFA pinning and key pair challenge that prevent the user from connecting to faked SSO portals and attackers can't initiate a connection cycle with the real portal IDP.

NIST 800-63

Impersonation Resistance

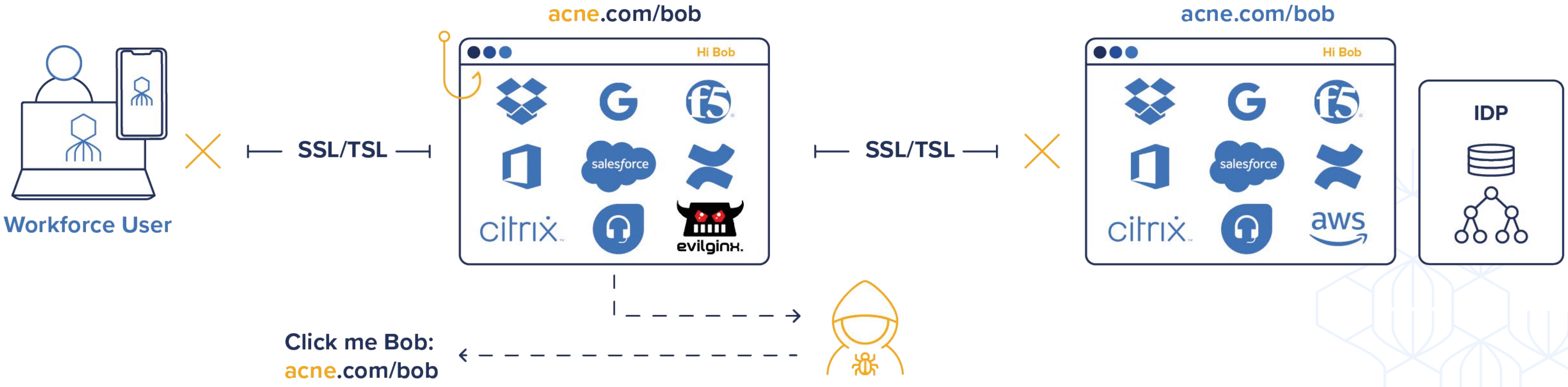
Replay Resistance

MITM Resistance

Several types of MITM exploits exist:

- Some campaigns involve **physical proximity**. Attackers create fake unsecured Wi-Fi hotspots in places like coffee shops. When patrons unknowingly connect, the would-be hacker in the middle gains access to data, including credentials and cookies.
- In other, **"man-in-the-browser" (MITB) attacks,** phishing emails prompt users to click links and install malware that records data sent between the victim's device and specific sites like company SSO portals or financial institutions. Phishers may also set up fake log-in pages — not difficult if you know how — and prompt users to log in and enter both credentials and OTPs.
- **SIM swapping:** Cybercriminals learn enough to impersonate users, answer security questions, and ask mobile carriers to reassign cell phone numbers to a new SIM card that lets them access victims' data remotely.
- **MFA prompt / push bombing / MFA fatigue attacks:** These social engineering attacks leverage the fact that MFA frustrates users by impersonating IT (and other legitimate entities) and bombarding users with verification prompts until they give in and approve the request.

Phishing-resistant MFA stops the start of push bombing and MiTM attcks

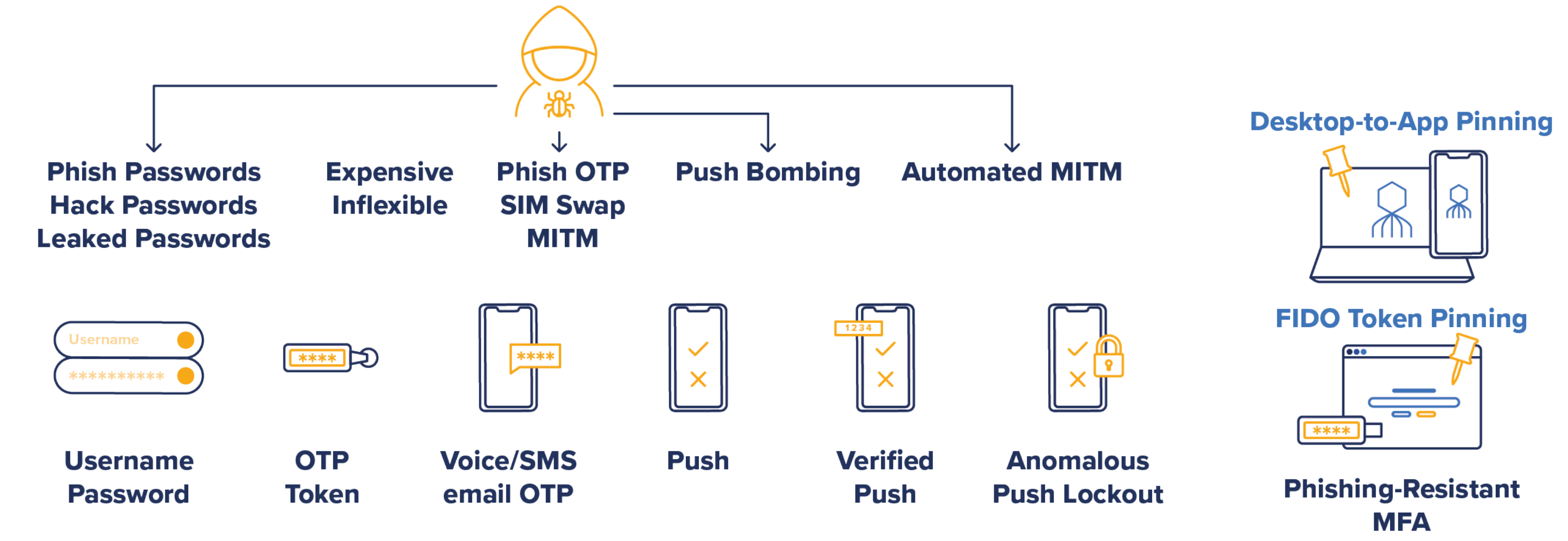


Heading hackers off at the pass

To resist phishing, users take FIDO tokens and register a set of PKI keys with the real site. The registration process links the username, the site's URL, and the keys together in such a way that anyone attempting to authenticate with a particular username would need to have the private key or token to decode the signed public key. This process also catches the slight, otherwise-easy-to-miss discrepancy between the real and fake URLs.

Along with the inherent benefits of passwordless, the Octopus Authenticator delivers a suite of phishing-resistant capabilities that work with password directories.

Evolution of Phishing Attack and Defense



Attack Strategy	How it Works	SDO Phishing Resistance Feature	What It Does
Phishing credentials	Hackers send email or use malware to trick users into providing credentials used to verify identity.	Removing passwords from user authentication.	Users can't share what they never know or have.
MFA attacks	Attacker exploits MFA weakness including bombarding users with push notifications and other push fatigue strategies.	Octopus adaptive MFA • Verified push. • Requester geolocation. • MFA retry timeout and lockout.	Upon detection of policy violation, Octopus presents additional information to the user and challenges to the requester. Incorrect responses initiate requester timeout and lockout responses. Phishing-resistant MFA pinning stops prevent the start of an MFA attack.
Advanced MITM phishing attacks	Hackers insert themselves between fake copies of target sites and the real sites. They record and hijack sessions or trick users into providing both credentials and PINs or OTPs used to access the real site.	SDO Phishing-resistant mobile push. FIDO2 token to FIDO2 Server key pair pinning.	Users sign into Mac, Windows or Linux desktops with the Octopus and access web and corporate apps with a single login workflow. Desktop-to-App pinning or FIDO2 token key pair pinning prevents unauthorized MiTM attacker from using URL redirection or fraudulently login to the real website.

Chapter 5:

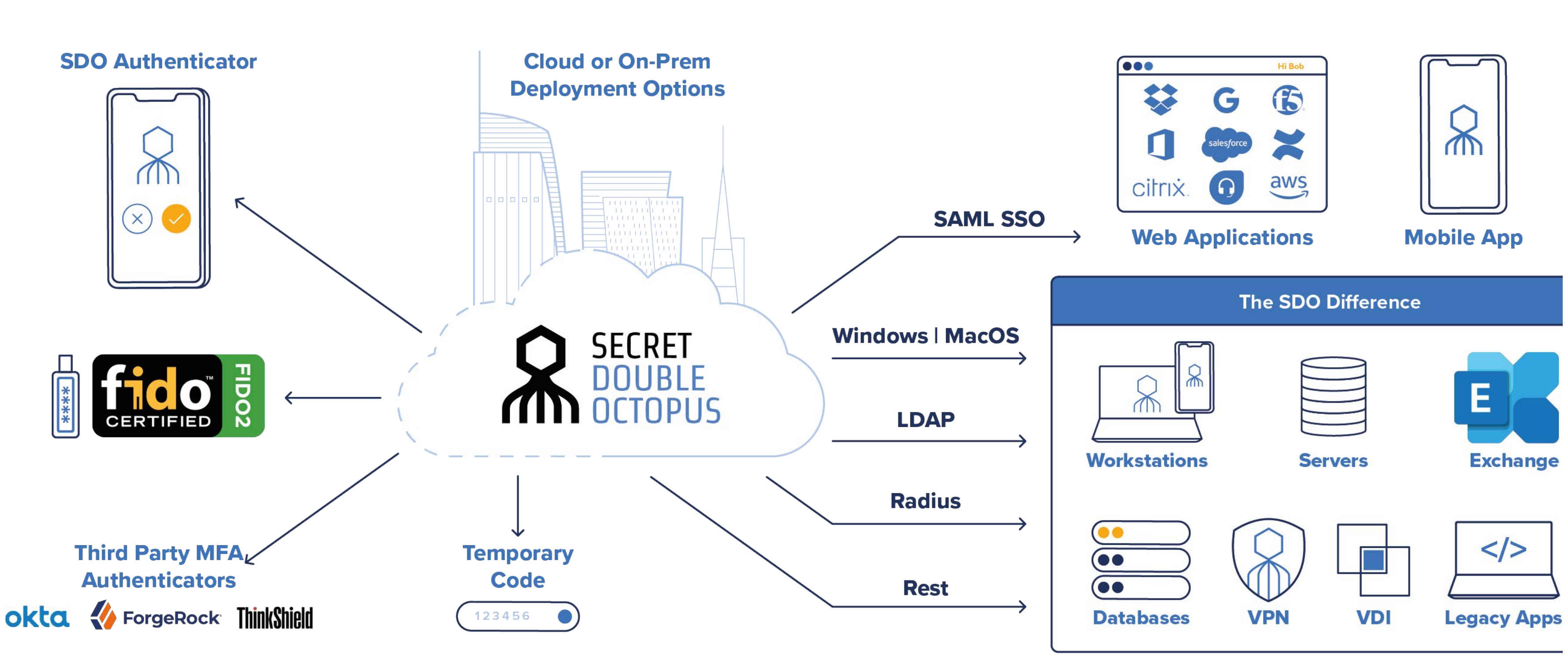
The Right Approach Keeps IT in Control

Why drop passwords as you add MFA?

A practical approach to phishing-resistant MFA:

- Delivers passwordless login in today’s password-centric world
- Takes passwords out of the user authentication process and password management out of users’ domain
- Improves UX and “ITX”
- Addresses all workforce use cases today
- Disrupts modern MITM attacks
- Maintains or expands IT control
- Supports FIDO2 with a clear path to PKI

Enterprise-wide Passwordless MFA



Change is hard. Octopus is easy.

SDO's approach eliminates passwords from the user experience to protect your business and satisfy the intent of Zero Trust mandates to become phishing-resistant. We offer the only solution that can do this today for all enterprise use cases while keeping IT in control of the journey to a PKI infrastructure.

SDO decouples users and backend infrastructure and uses FIDO, PKI, and desktop-to-app signed pinning to streamline authentication and stop phishing from costing you millions. Our approach achieves the full promise of passwordless MFA — reduced risk, cost, friction, Help Desk calls, and phishing. No passwords with no change.

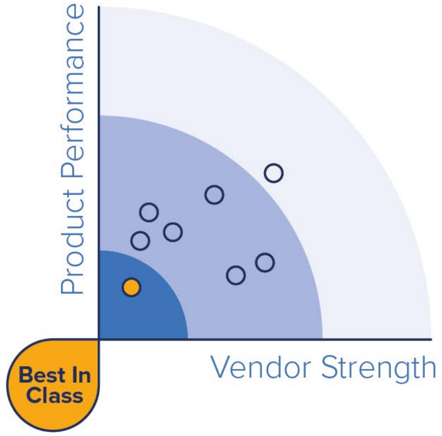
Curious?

Run your own information through the Passwordless MFA ROI Calculator to see what you stand to save.

SDO is Industry Proven

SDO Chosen as “Best in Class” in Enterprise Passwordless

2021 Aite Group Enterprise Passwordless Authentication Report



“SDO earns higest honors… because of its range of features, rich integration capabilites, excellent user experience, and very high cumstomer satisfaction.”

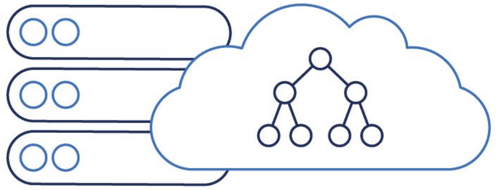
SDO is Most Complete

Complete: Enterprise-wide use cases		Certificate only Passwordless Vendor
Desktop	●	◕ *
Apps (cloud & mobile)	●	◕ **
FIDO2	●	◑
VDI	●	●
VPN	●	◕
Admin (RDP/SSH)	●	●
BYOD	●	●
Legacy	●	◔
Offline (airplane, etc)	●	◕
Airgap (critical infra)	●	○

* No MAC Filevault
** No SSO Portal

Change is Hard, SDO is Easy

Works with Password Directories



No Changes Needed

Takes about an hour to start onboarding users

Resources

1. https://www.prnewswire.com/news-releases/slashnexts-state-of-phishing-report-reveals-more-than-255-million-attacks-in-2022-signaling-a-61-increase-in-phishing-year-over-year-301659518.html
2. https://www.ibm.com/downloads/cas/3R8N1DZJ
3. https://go.doubleoctopus.com/ponemon-workforce-authentication-report
4. https://www.bbc.com/worklife/article/20161219-tech-issues-kill-productivity-but-dont-rush-to-call-it

https://www.prnewswire.com/news-releases/multi-factor-authentication-market-2023-2027-a-descriptive-analysis-of-parent-market-five-forces-model-market-dynamics--segmentation---technavio-301685312.html

https://www.globenewswire.com/en/news-release/2021/09/07/2292170/0/en/Global-multi-factor-authentication-market-to-reach-40-00-billion-by-2030-Allied-Market-Research.html

https://www.prnewswire.com/news-releases/multi-factor-authentication-market-2023-2027-a-descriptive-analysis-of-parent-market-five-forces-model-market-dynamics--segmentation---technavio-301685312.html

https://ransomware.org/how-does-ransomware-work/active-defense-intrusion/phishing-attacks/

SECRET
DOUBLE
OCTOPUS

Secret Double Octopus is a leader in workforce passwordless and MFA solutions. It's industry-leading Octopus authentication platform offers mid-market to Fortune 100 enterprises the ability to move to a higher security, more frictionless future progressively, from MFA to end-to-end, unified passwordless authentication. From leveraging existing MFA authenticators to supporting legacy on-premise applications, no other desktop MFA and enterprise passwordless platform offers as much robustness and flexibility as the Octopus solution. The company has been designated a Gartner "Cool Vendor" and more recently named "Best-in-Class" passwordless solution by AITE Group in 2021.

Learn more at **doubleoctopus.com**