E-BOOK

5 Reasons

Financial Organizations Are Modernizing MFA

SECRET DOUBLE OCTOPUS

Table of Contents

“Access management solves multiple challenges at once.”

IT leaders in financial services have their work cut out for them with mergers and acquisitions (M&A) workforce unification, digital transformation, and an endless stream of regulatory mandates to meet – and surprisingly few technologies able to help on all fronts. As cybersecurity’s new “perimeter,” access management solves multiple challenges at once.

In this book we’ll look at 5 ways that innovations in multi-factor authentication (MFA) deliver higher ROI, stronger security, and greater scale and agility. The process starts with removing user passwords from the login process and making it harder for threat actors to phish users and launch attacks.

We’ll see how the ideal approach to passwordless MFA:

1. **Avoids cyber risk from phishing, ransomware, and account takeover (ATO)**
2. **Speeds M&A integrations**
3. **Modernizes cybersecurity and compliance for legacy applications and systems**
4. **Meets Zero Trust mandates to reduce liability and insurance premiums**
5. **Saves IT lots of work and bring in millions of dollars of ROI per year**

As an added bonus, the Secret Double Octopus Passwordless MFA platform delivers a better, faster user experience (UX) as employees authenticate into their company’s systems anywhere and everywhere.

Chapter 1

Change Is Making Passwords a Thing of the Past - Faster Than You Might Think

Modern cybersecurity authorities and best practices recognize the value and importance of improving user identity assurance and stopping phishing. NIST, CISA, MITRE ATT&CK – anything rooted in a zero trust philosophy – all specify a need for phishing resistance to stop malware, ransomware attacks, data theft, outbound attacks on supply chains, and insider threats.

The Anti-Phishing Working Group (APWG) observed almost

5M

phishing attacks over the past two years

Phishing attacks grew

>150%

per year in recent years (APWG)

MFA as we know it falls short

Guidelines typically specify using MFA to verify that the person asking to be let into the system has a recognized and trusted device (like a hardware token or a cell phone) and/or possess the right fingerprint, voice, or facial characteristics. The goal is to avoid relying on passwords alone—which is good—but not good enough.

When all is said and done, keeping passwords as the first factor of authentication renders MFA inherently fallible.

A passwordless approach eliminates risk—and aggravation

Users get confused—and annoyed—dealing with siloed access to the resources they need and managing a bunch of different passwords and second-factor authenticators. Instead of just piling more steps into the process, removing user passwords as the first factor makes authentication workflows stronger, faster, and simpler.

A passwordless approach takes away attackers' favorite tool—phishing—while increasing confidence that the person attempting to log in is a legitimate user looking to do only legitimate things.

High assurance starts at the desktop

Anyone can stroll into a cubicle and log into a PC using a password taped to the monitor. Getting rid of passwords and incorporating the two stronger pillars of identity verification — something users have and something users "are"— all but eliminates that impersonation and social engineering risks. From there, financial services organizations need to extend secure login to shared workstations and accounts, legacy servers and systems, cloud workloads, and perhaps above all, remote access.

A passwordless approach eliminates:

- The 80+% of breaches that involve compromised credentials
- Phishing, modern phishing-as-a-service (PhaaS), and man in the middle (MITM) attacks
- All doubt that those responsible for security did everything possible to avoid credential compromise abuse of trust

Passwordless is easier than it sounds

Most IT and identity and access management (IAM) leaders already know that getting rid of user passwords makes their security practice much stronger. And that, once the migration takes place, users will love the simplified login workflows.

What may be less obvious — and the reason every company hasn't made the change yet—is that getting rid of passwords can be quick and easy, and that it can mean less work for IT operations teams.

Why passwordless?

A passwordless approach leverages the strongest factors of identity verification – "what users have" and "who users are" — instead of vulnerable secrets that can be lost, leaked, sold, and stolen.

A passwordless login takes away attackers' favorite standby tactic — phishing for user credentials to gain initial access — as well as modern options like buying credentials on the black market.

Chapter 2

Can MFA Speed M&A?

Financial services isn't the only sector that uses mergers and acquisitions to fast-track growth, but it very well may face the greatest challenges in consolidating workforces. A succession of mergers creates a gnarly mass of fragmented identities, login workflows, and IAM platforms—some more outdated than others. At the same time, consolidation makes for an ideal time to centralize and standardize around a single unified login.

Two paths to streamlining the login process

Two or more merging companies may use multiple IAM solutions like Okta, Ping, and Entra ID or the other dozens of vendor options to access applications and Active Directory to manage identities on the back end. Standardizing on one approach eliminates the disjointed workflows that give rise to visibility gaps, a confusing user experience, and complex audit trails.

How IT approaches the merging of two workforces impacts speed, effort, and cost, and whether "one plus one" produces a force-multiplying gain. Workers from both organizations need a streamlined mechanism to access the combined apps and infrastructure. How IT approaches the merging process has a dramatic impact on time, effort and cost.

> "'Transformation is continuing to drive M&A activity across financial services—although in response to economic challenges, I see dealmakers using smaller transactions to achieve more transformational steps towards digitalisation, ESG, and portfolio optimisation."
>
> Christopher SurGlobal Financial Services Deals Leader, Partner, PwC

Consolidation is a matter of time — and effort in achieving the unification programs goals

Integration Goals	Universal IAM MFA	Unified MFA with heterogeneous directories
Unified login workflow for the entire workforce	After all users and apps have been migrated to a single IAM (months, years)	Immediate
Security goals achieved	After all users and apps have been migrated to a single IAM (months, years)	Immediate
User experience goals achieved	Gradual, until all user and apps have been migrated to a single IAM	Immediate
Single source of truth achieved (universal IAM)	Months, years, or never achieved	Not immediate. IT can modernize backend identity infrastructure faster without user secret coordination

Universal IAM

Larger IAM vendors propose a “universal IAM” approach. Transitioning the acquired entities’ applications, directories, and identity infrastructures to the acquiring company’s IAM platform sounds simpler in theory but may chart a path forth with obstacles and incompatibilities.

Phased migrations take months, years, may never get completed

Time is the enemy of workforce unification.
The “universal IAM” approach requires all managed resources from all identity platforms to be refitted to match the requirements of the prevailing IAM platform. IT may need to recode applications or build custom connectors to support the universal IAM vendor’s single sign-on (SSO) and FIDO2 technology — and some convert more easily than others.

On average, retooling a single application to work with a new IAM takes a well-staffed team, 5-7 days in the best case. For financial services organizations maintaining thousands of apps—including many custom and legacy services that can’t be updated at all—consolidation could take months, years, or might never achieved 100% coverage.

Morgan Stanley recently predicted that ‘deal-making’ would accelerate throughout and beyond the coming years, driven by:

- Well-capitalized companies making acquisitions in their core businesses
- Financial sponsors, which are holding record amounts of capital, deploying it in acquisitions
- Uneven performance among companies stoking shareholder
- Cross-border M&A making a comeback

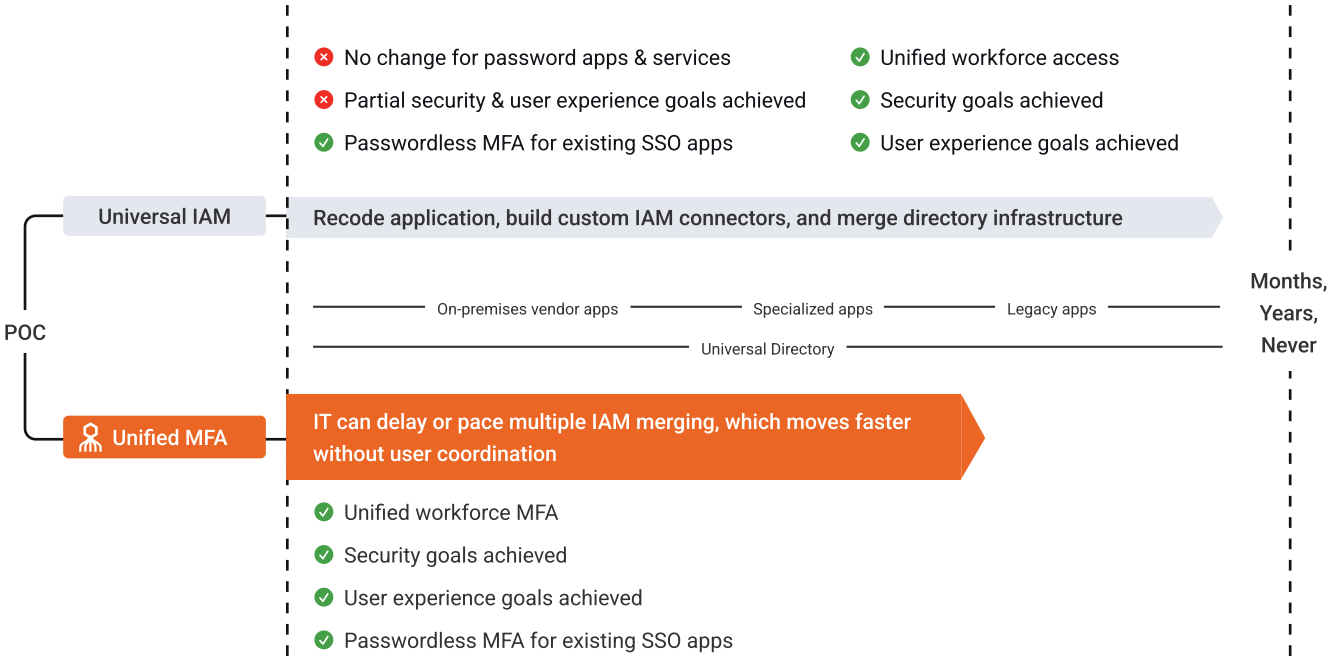
Unified MFA benefits for the blended workforce

Compared with choosing and migrating to a single IAM solution, Secret Double Octopus delivers the same security benefits and streamlined user experience, only faster. By migrating the MFA portion of the login process to the Octopus platform adds a flexible passwordless authentication layer that works with any existing IAM platforms and allows IT to migrate users from one to the other without recoding applications or directories.

Octopus decouples user login from identity infrastructure to give IT full control over upgrades. The platform works with all leading vendor IAM platforms, including on-premises Active Directory and multi-vendor platforms.

Businesses can accelerate workforce consolidation and tackle identity infrastructures whenever IT chooses.No more secrets to manage!

The Same Outcome - Very Different Timelines



Enterprise-wide use case coverage takes hours to start, days to finish

Blended workforces typically support a range of Windows, Macs, Linux, legacy and custom systems. Windows Hello for Business (WHfB) only works with some-not-all Windows platforms. FIDO2 technology only works with web-based resources

Unlike other solutions — even other passwordless approaches—Octopus provides enterprise-wide use case coverage for on-prem, remote and cloud applications. All applications can be migrated quickly and easily instead of one-by-one so companies growing by acquisition can quickly integrate new workforces and tightening controls as they go.

	SSO	Windows	Mac	VPN	RDP	VDI	Linux SSH	Non-AD (DB)	AD-joined	On-prem	Air Gap	Shared Accounts
SECRET DOUBLE OCTOPUS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WHFB	✓	✓	—	—	—	—	—	—	—	—	—	—
fido	✓	—	—	—	—	—	—	—	—	—	—	—

Figure 2. Octopus delivers enterprise-wide passwordless MFA use case coverage

Chapter 3

Modern Security for Legacy Apps

Consumers barely react to breaches at retail giants like Target and Home Depot, but it's a different story when it happens to banking institutions. Along with compliance, the heightened focus on protecting customer data leads financial services institutions to store privileged data onsite instead of migration to public cloud services.

"If it ain't broke, don't fix it"

Storing data on legacy server infrastructures, and even some old mainframe computers within data centers may be safer, but maintaining older systems brings its own challenges. The talent pool of experts versed in older technologies shrinks every year and companies hesitate to disrupt complex infrastructures that predate the current team.

> Finance holds itself to higher standards – and it worksA recent a recap of 2023 attacks on financial services organizations by ThinkAdvisor found the top 12 attacks on financial services companies exposed roughly 35M accounts combined — less than half than of just one 2023 healthcare provider breach that affected more than 88M.
>
> (Source: ThinkAdvisor, 12 Biggest Financial Services Data Breaches of 2023)

"On-prem" doesn't always mean "old"

Bloomberg reported that 54% of all new applications are being deployed locally versus in the cloud. A study by Dimensional Research showed 92% of companies said on-prem software sales were growing.

Applications running on-prem behind firewalls need the same caliber of authentication protection as those exposed publicly through the cloud—if not more—especially at sites where contractors, suppliers, and disgruntled insiders are likely to be accessing systems. Besides keeping data where IT can see and control it, continuing to run applications on already-paid-for systems reduces costs associated with network and cloud service utilization. While doubling down on data center operations, companies must find new ways to strike the balance between digitalization, security, and user experience—a formidable challenge when:

New IAM technologies focus on the cloud

Most IAM strategies, and even most MFA solutions, heavily target cloud and Web-based applications. Because cloud-focused IAM solutions offer no viable alternative to using Active Directory to manage identities on the backend, most leading IAM solutions can't protect legacy and custom applications.

Partial use case coverage leaves enterprises at a loss to deliver a unified high-assurance login for all remote and local users, and maintaining redundant systems drives up cost, skills requirements, and the burden on Help Desk teams. Instead of reducing risk, the added complexity can delay the progress and/or benefits of M&A, digitalization, and other transformation initiatives.

Passwordless MFA upholds a legacy of trust

Octopus Passwordless MFA reconciles the tension between leveraging modern cloud services and maintaining essential operations on-premises with two essential advantages:

A safe, simple, unified login

Octopus protects access everywhere, anytime from desktops (with or without SSO) to on-premises apps and the cloud. Login workflows feature biometrics and user-preferred mobile push to reduce login times by 70% – with fewer steps for users to take.

Complete use case coverage to stop phishing

SDO works with any application on the front-end and with any IAM or directory infrastructure behind the scenes.

A forward-looking IAM strategy:

- Highest-assurance authentication for web, cloud, and on-premises custom and legacy applications
- Unified login experience for all workers and authorized third parties
- Streamlined compliance and backend operations

Chapter 4

Passwordless Meets Zero Trust Mandates

Data may be safer onsite, but compliance could still be at risk. Older systems might not support newer technologies and zero-trust policies aimed at elevating cyber, and sometimes national security.

In the U.S., the updated NYDFS Cybersecurity Regulation mandates that all organizations operating in New York implement phishing-resistant authentication by 2026.
Other countries have issued similar policies that extend to financial institutions working with national governments.

Along with potential fines, breaching compliance can mean losing government contracts, reputational damage, and having to pay higher cyber insurance premiums.

The CISO's new dilemma: "Did we do enough to stop a breach?"

Ninety percent (90%) of data breaches still start with a phish and MFA hasn't stopped phishing. Neither has education despite the fact that companies invest millions in phishing awareness training

The boxes get checked, and the phishing goes on, because making it the user's responsibility.

And now the use of AI in socialengineering, commercialized email wizards, PhaaS, and automated manin- the-middle (MITM) attacks can turn even novice attackers into formidable adversaries while making it harder for users to recognize phishing expeditions.

4.6%

Of users clicked the bait, even after one year of cyber training

54.1 Million

Phishing security tests

11.9 Million

Users

55.7 Thousand

Organizations

KnowBe4, 2024 Phishing Industry Report

Who's Gets Held Accountable?

In 2021, the Federal Trade Commission (FTC) updated its Safeguards Rule to require nonbanking financial institutions like mortgage brokerage firms and payday lenders to limit who can access consumer data, add encryption, and explain information-sharing policies. The same year, **TikTok** and Facebook both paid large sums- $92M and $650M respectively—to settle class-action lawsuit alleging the companies failed to comply with Illinois' **Biometric Information Privacy Act (BIPA)**.

Compliant doesn't mean secure but passwordless MFA does

Every cybersecurity best-practice checklist calls for MFA, but guidelines for implementation aren't always clear:

- The EU financial services directive, the Digital Operational Resilience Act (DORA) Article 9 says companies must, "Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems."
- The prescriptive CIS Critical Security Controls V8 that affects many financial services enterprises specifies MFA should protect Internet-facing, remote, and privileged users but that doesn't prevent imposters from masquerading as trusted users or inhibit access to PCs used at branch locations.
- PCI DSS details Qualified Security Assessor (QSA) official Report on Compliance (ROC) and you could pass every item—but—if a CHD security incident occurs, companies officially become out of compliance.

Following a breach, penalties (and next year's insurance premiums) may hinge on subjective assessments of whether security leaders did enough to stop it from happening. One definitive doctrine, the NIST 800-63 (Digital Identity Guideline) spells out requirements for high assurance MFA based on the potential harm a failed authentication might cause to an organization and its stakeholders.

	Impact of failed authentication	Maximum impact to safety	Acceptable authentication methods
AAL1	Low	None possible	Username & password SMS/email OTP MFA
AAL2	Moderate	Low	Mobile push notifications OTP tokens
AAL3	High	Moderate or high	High assurance authentication

NIST 800-63 radiates out to enterprises that do business with governments and industries subject to NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) regulations.

Government-caliber identity verification

With its recent announcement of AAL3-compliant identity verification, SDO delivers the industry's highest-assurance, phishing-resistant MFA for highly regulated industries. Businesses can achieve phishing-resistance across their entire workforce while maintaining the sanctity of specialized, custom applications and systems onsite.

In keeping with zero trust, AAL3 aims to assure security teams that the requester is who they are. Passwordless MFA removes the risk of credentials being stolen, shared, or hacked, or the simple second factor used to verify identity being obtained via social engineering. Octopus passwordless MFA combines NIST AAL3 cryptographic binding of the "something you have" to what is being accessed, and then with the "something you are" to create the highest possible identity assurance.

'Did we do enough?'

Adopting passwordless MFA helps make the case that companies did everything in their power to prevent and neutralize attacks based on compromised credentials and identities. Continuing to use passwords clearly proves they did not.

Phishing-resistant characteristics	Passwordless MFA	Traditional MFA
Impersonation resistant	✓	✗
Social engineering resistant	✓	✗
MITM resistant	✓	✗

Traditional MFA does not deliver phishing resistance, nor does it qualify as "best practice" security. Only a passwordless approach takes the human factor out of the authentication equation by using the stronger "what you have" and "what you are" criteria for verifying identity.

Octopus also uses cryptographic binding to pin users, apps, and authenticator together. Users prove who they are; no judgments to make, no passwords to remember, or no manipulatable actions to avoid, relieving employees from phishing sentry duties.

Chapter 5

High-Assurance MFA Makes Dollars and Sense

The financial services industry—every industry—will eventually adopt a phishing-resistant, passwordless approach to MFA – it's a question of 'when' not 'if.' Octopus Passwordless MFA improves ROI and pays for itself in the first year as:

- **Employees become 5% more productive** as removing the time-consuming foundational step of entering passwords streamlines workflows.
- **IT avoids up to 40% of all Help Desk calls** and allhands- on-deck quarterly password rotation cycles.
- **Phishing-resistance eliminates 80%+ of risk** on day one.
- **Positively impacts cyber insurance premiums** by aligning with zero-trust recommendations from CISA, NIST, MITRE ATT&CK and others.
- **High assurance MFA meets NIST AAL3** requirements for desktop MFA.
- **Users begin onboarding in an hour** and IT completes rollouts in days.

A BBC study suggests employees can save up to

22 mins/day

5% of a typical workday

See the Octopus ROI calculator

Alejandro Leal, lead passwordless analyst at KupplingerCole defines passwordless authentication this way:

> "Passwordless Authentication solutions should provide a consistent login experience across all devices, introduce a frictionless user experience, include an integrated authentication approach, and ensure that no passwords or password hashes are traveling over the network anymore."

It is a good definition, however at Secret Double Octopus, we believe enterprises need additional criteria for an effective solution:

- All workforce users have a single access workflow to all enterprise applications and services
- One experience across the whole hybrid enterprise while making workers' and admins' lives better

Choosing the ideal solution

In evaluating the right solution, IAM and security leaders should ask:

Does the solution deliver complete use case coverage?

Octopus meets the full gamut of enterprise authentication needs – desktop, legacy apps, secure remote access, and physically challenging environments

Does it stop phishing?

Passwordless MFA has the potential to thwart impersonation, SIM swapping, man-in-the-middle (MITM), and MFA push-bombing attacks. The Octopus platform includes a phishing-resistance feature suite that meets requirements outlined NIST and CISA.

Is the approach budget-friendly?

- Will IT need to purchase, ship, and maintain new hardware tokens or other physical authenticators?
- Will the solution increase or decrease calls to the Help Desk?
- Will it streamline or complicate compliance audits and reporting?
- How much of the application and directory infrastructure will need to be updated to implement this passwordless approach?

Does the solution offer the highest-assurance identity verification?

AAL3 means higher assurance than AAL1 and 2, so companies assume achieving that level of security must be harder and more expensive. But with Octopus's passwordless MFA, very little work isrequired by IT to achieve high assurance, with or without hardware tokens.

Does it move us closer to Zero Trust?

M&A, MFA, and passwordless can be three separate journeys—or a single investment can help you move forward with all three. Octopus unifies MFA, strengthens security improvements, and delivers a better user experience with substantially lower effort and expense than universal IAM. Broad use case coverage and deployment flexibility make it faster and easier to onboard additional groups throughout future M&As and other growth strategies as business priorities change.

Does it move us closer to Zero Trust?

M&A, MFA, and passwordless can be three separate journeys—or a single investment can help you move forward with all three. Octopus unifies MFA, strengthens security improvements, and delivers a better user experience with substantially lower effort and expense than universal IAM. Broad use case coverage and deployment flexibility make it faster and easier to onboard additional groups throughout future M&As and other growth strategies as business priorities change.

Does it stop phishing?

Passwordless MFA has the potential to thwart impersonation, SIM swapping, man-in-the-middle (MITM), and MFA push-bombing attacks. The Octopus platform includes a phishing-resistance feature suite that meets requirements outlined NIST and CISA.

Is the approach budget-friendly?

- Will IT need to purchase, ship, and maintain new hardware tokens or other physical authenticators?
- Will the solution increase or decrease calls to the Help Desk?
- Will it streamline or complicate compliance audits and reporting?
- How much of the application and directory infrastructure will need to be updated to implement this passwordless approach?

Does the solution offer the highest-assurance identity verification?

AAL3 means higher assurance than AAL1 and 2, so companies assume achieving that level of security must be harder and more expensive. But with Octopus's passwordless MFA, very little work is required by IT to achieve high assurance, with or without hardware tokens.

SECRET DOUBLE OCTOPUS

About Secret Double Octopus.

At Secret Double Octopus, we believe authentication should be stronger, simpler, and completely password-free.

Our patented ZeroPassword™ technology eliminates passwords even from legacy and on-prem systems, delivering unmatched security and user experience.

Our platform integrates seamlessly into any infrastructure, supporting any system, use-case, or authentication method.

Trusted by SMBs and Fortune 500 enterprises alike, we secure billions of authentications annually, enabling organizations to achieve modern, phishing-resistant security at scale.

Learn more at doubleoctopus.com **Get a demo**

Trusted by the world's most heavily regulated organizations.

Weil · TELUS · tinsa · 3M · VEOLIA · standard chartered · PRUDENT · RBC Royal Bank · BNP PARIBAS · Cleveland Clinic · PENNYMAC FINANCIAL SERVICES