Solution Overview

ZeroPassword™

for Financial Services

Eliminate legacy passwords with a universal phishing-resistant MFA

SECRET DOUBLE OCTOPUS

Solution highlights

Enterprise-wide universal MFA coverage including legacy apps

Compatible with existing apps and directories without redesign

Zero-trust authentication meets NIST AAL3 requirements

Future-ready with patented post-quantum resilience

Suite of end-user phishing-resistant authentication methods

Audit-ready trail for all authentication related events

The unique challenges of financial organizations

IT leaders in financial services are facing a growing list of pressures: a patchwork of authentication methods across the IT stack, legacy systems that can't integrate with modern IAM, auditors flagging MFA coverage gaps, and mounting scrutiny from management and boards in the wake of breaches and compliance fines headlines. And then there's the real threat driver: phishing and ransomware, which thrive on identity weaknesses, especially in finance.

You've heard the "go passwordless" answer before. But most approaches run into the same limitations: they work only for modern, SSO-integrated applications, or they deliver a shallow "passwordless experience" that shifts risk around and often makes things worse.

ZeroPassword™ changes that- easily.

Select regulations and best practices addressing digital authentication

Financial Regulation / Guidance	Digital Authentication Requirements
NYDFS - 23 NYCRR Part 500 Cybersecurity Requirements	Starting November 1st 2025, all covered entities are required to use MFA for any individual accessing any of its information systems
FFIEC Guidance	- Strong authentication for high risk users - Protect remote access software with MFA
National Credit Union Administration (NCUA)	Relies on FFIEC guidance as a benchmark for effective risk management principles and practices, including MFA for high risk and remote access
PCI DSS 4.0 Payment Card Industry Data Security Standard	After March 31, 2025 MFA is required for all accounts accessing cardholder data, not just administrators
NIST 800-63 - Digital Identity Guidelines	Authenticator Assurance Level AAL3 for high risk situations requires phishing resistance and verifier compromise protections
FINRA - Best Practices	Use MFA for login access to the firm's systems accessed by staff, contractors and customers

Eliminate passwords, don't just hide them

Eliminating passwords - and, in turn, phishing threats - meets today's standards for zero-trust identity and improves your employees' login experience. To get there, enterprises need seamless integration with existing infrastructure, allowing IT to modernize workforce authentication processes without disrupting existing systems.

While other solutions claim to be passwordless but really just mean using passwords less often, Octopus delivers an elegant solution for eliminating passwords from users' login experience completely. The platform works with any application and with your existing identity infrastructure without requiring costly efforts to recode applications or rearchitect directories to match IAM vendor requirements.

Users never need to create, remember, type, or expose another password ever — that's passwordless!

Enterprise-wide use case coverage

Octopus Passwordless MFA modernizes user-authentication while working with modern SSO, FIDO-ready apps and existing password-based apps and directories out-of-the-box. Unlike other passwordless MFA solutions that only work with Windows desktops and apps covered by SSO, the Octopus platform provides complete enterprise use case coverage so you can eliminate user passwords while securing every IT-managed app and service. Octopus even works with standalone apps with access control lists embedded in databases that are not joined to directories.

To achieve maximum coverage with minimal disruption, Octopus converts user passwords to ephemeral machine-generated tokens used to orchestrate secure access to every IT-managed application and service. IT achieves a streamlined, phishing-resistant MFA that pays quantifiable business dividends in a fraction of the time it takes using other vendor methods.

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

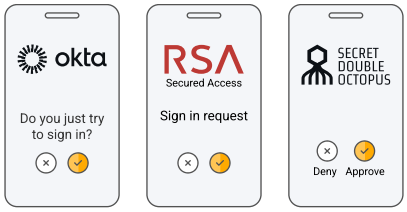
ZeroPassword™ MFA features

- Fully featured SSO portal for Web / mobile apps
- Password elimination for:
  - Windows & Mac (including FileVault)
  - Password-based legacy apps & on-prem DBs
  - Shared and service accounts
  - Any VPN, VDI & RDP use-case
  - Air-gapped systems
- Universal authenticator compatibility (apps, FIDO, smartcard etc)
- OTP & offline fallback options
- The only smartphone based NIST AAL3 compliant authenticator
- Workstation-to-app pinning

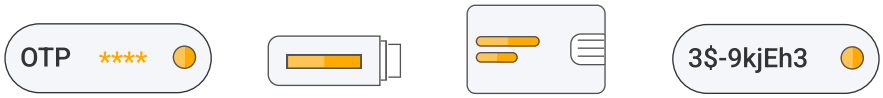
Unique Octopus benefits

Keep your authentication method

Enterprises with diverse workforces need the flexibility to choose the most appropriate end-user authenticator. Octopus offers the broadest range of high-assurance authentication methods so you can achieve more coverage fast with less disruption to user workflows.



Third-Party | Octopus



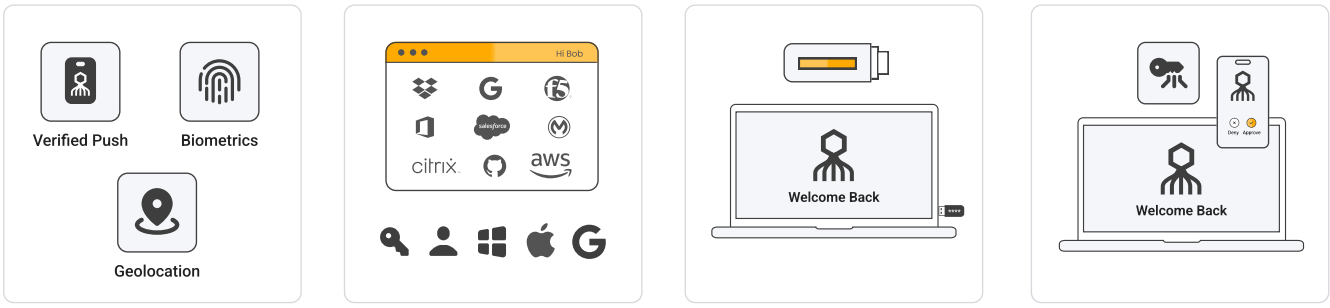
OTP | Passkey | Smartcard | Temporary Token

SSO now covers legacy apps too

SSO from Identity Providers (IDPs) makes login more secure and user-friendly, but they only cover web apps. Octopus delivers the industry-only SSO for legacy and homegrown apps.

Modernize legacy and on-prem authentication

Many enterprises rely on mission-critical self-managed, custom, and legacy apps that run on-prem. Only Octopus delivers passwordless authentication to these legacy password-based applications without a costly redesign.



Adaptive | Synced Passkey | Device-bound Passkey | Octopus Desktop-to-App pinning

Simple governance of heterogeneous directories

M&As and steady business growth leave enterprises with multiple user directories and IDPs. Octopus simplifies work in heterogeneous environments, and unifies admin and user experience with one secure passwordless MFA workflow.

Secure remote access - even inside air gaps

Octopus lets IT enforce user friendly, passwordless MFA for secure remote access and inside internet-isolated demilitarized zones (DMZs) and jump servers protected within physically isolated air gap environments.

Bullet-proof phishing-resistance

FIDO is great because it is phishing-resistant, but it only works with web apps, and enterprises run on more than web apps. Octopus provides the same level of phishing-resistance to universally cover all IT-managed apps and services, including legacy apps

Protect shared accounts

Account sharing complicates every security, compliance, and cyber insurance test but remains a common practice for frontline shift workers and IT administrators. Octopus provides visibility and auditing for each worker's access as they share resources without forcing a hefty redesign.

Minimize employee downtime

Provide white-glove IT service to employees by allowing technical staff to share the end-user's computer profile temporarily, with a clear audit trail so IT can fix problems with minimal disruption to employee schedule.

How it works

The Octopus Authentication Platform is built around a patented technology that eliminates every user-managed password across the IT stack, replacing it with machine-generated ephemeral token the user never knows.

Employees get a unified authentication flow across their apps and services, using FIDO2, passkey, smartcards, OTP tokens, or mobile push. Once the user has completed high assurance authentication, Octopus logs them in to the requested service without a need to use a password.

SECRET DOUBLE OCTOPUS

About Secret Double Octopus.

Secret Double Octopus delivers the industry's broadest workforce use case coverage for passwordless MFA making SDO a clear leader in phishing-resistance, enabling compliance, and reducing cyber insurance premiums. Our industry-leading platform offers mid-market to Fortune 100 enterprises the ability to progressively move to a higher security, more frictionless authentication – from MFA to end-to-end, unified passwordless authentication.

From leveraging existing MFA authenticators to supporting legacy on-premises applications, no other desktop MFA and enterprise passwordless platform offers comparable robustness and flexibility. The company has been designated a Gartner "Cool Vendor," named "Best-in-Class" passwordless provider by AITE Group and a 2023 SINET16 Innovator.

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