SECRET DOUBLE OCTOPUS

SOLUTION OVERVIEW

Octopus Passwordless MFA

The industry's most complete passwordless MFA solution for your workforce

Solution Highlights

- Suite of Phishing-resistant methods
- Enterprise-wide passwordless use case coverage — including legacy apps
- Compatible with existing apps and directories without redesign
- Zero-trust identity verification meets NIST AAL3 requirements

“Passwordless” must mean no passwords

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!

> “From the moment of receiving a brand-new computer to becoming active, I have never worked with an IAM solution that was seamless and automatic to onboard”
>
> Director of IAM, RTX, formerly Raytheon Corporation

The only solution for 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.

	Cloud/ Mobile SSO	Windows Desktop	Mac Desktop	Remote VPN	Remote RDP	Remote VDI	SSH	Self-Managed On-prem	Legacy Apps: Directory joined	Legacy Apps: Stand -alone	Shared Accounts	Industrial/ Air Gap	Eliminates all user passwords
FIDO	●	○*	○	○	○	○	○	○	○	○	○	○	○##
WHfB	●	●	○	◐•	◐#	○	○	○	○	○	○	○	○##
SDO	●	●	●	●	●	●	●	●	●	●	●	●	●

*Requires WHfB & Entra joined

•No Radius VPN

#Only works with certificates

##Fallback & un-supported use cases

Octopus-Only Capabilities

1. Support all desired authenticators
2. SSO for web apps and legacy password apps
3. Modernize legacy and on-prem authentication
4. Integrate easily with heterogeneous directories
5. Secure remote access (SRA) — even inside air gaps
6. Suite of phishing-resistant MFA methods
7. Extend MFA to shared account resources
8. Roll out White-Glove Support services

1 Support all desired authenticators

Enterprises with diverse workforces need the flexibility to choose the most appropriate authentication method for each job function. Octopus offers the broadest range of high-assurance authentication methods so you can achieve more coverage faster with less disruption of user workflows.

2 SSO for web apps and legacy password apps

SSO from Identity Providers (IDPs) makes login more secure and user-friendly, but most SSOs start with passwords. Octopus integrates its own SSO web portal, makes your existing IAM vendors SSO passwordless, and delivers an industry-only Octopus Desktop SSO for password-based apps.

3 Modernize legacy and on-prem authentication

The majority of 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.

4 Integrate easily with heterogeneous directories

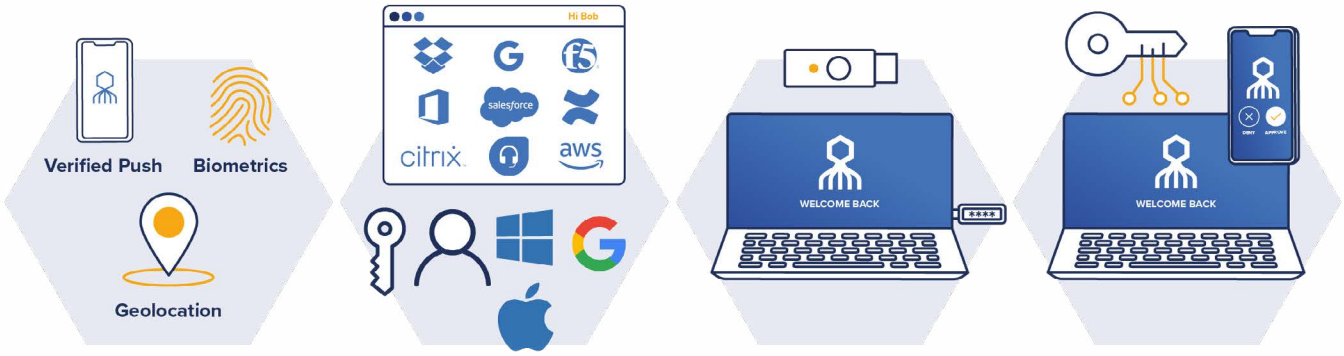
Mergers, acquisitions (M&As) and steady business growth leave enterprises with multi-vendor directory infrastructures and Active Directory as the source of truth. Octopus works seamlessly with heterogeneous directories and unifies the user experience with one secure passwordless MFA workflow.

5 Secure remote access (SRA) — even inside air gaps

Businesses that physically wall off valuable data and infrastructure still may need to enable and secure remote access. Octopus NIST AAL3-compliant authentication slashes companies' digital attack surface by getting rid of passwords to block attacks targeting traditional MFA. Octopus even 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.

6 Suite of phishing-resistant MFA methods

FIDO is great because it is phishing-resistant, but it only works with web apps, and enterprises run on more than web apps. Octopus extends FIDO2 usability to all IT-managed apps and services, including legacy apps. With the Octopus, IT can distribute hardware tokens or leverage lower-cost tokenless phishing-resistant Octopus mobile push, synced passkeys, and adaptive MFA.



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

7 Extend MFA to shared account resources

Sharing accounts fails every security, compliance, and cyber insurance test but remains a common practice for frontline shift workers and IT administrators. Octopus creates high-assurance MFA for each worker's access as they share resources without forcing a hefty redesign.

8 Roll Out White-Glove Support services

No one, especially executives and 'time is money' account reps, can afford to sit in front of their computer to take part in IT support sessions. Octopus lets approved technical staff share the service client's computer profile temporarily (and provides a clear audit trail) so IT can fix problems while executives sell and run the company.

Awarded the most robust passwordless MFA solution for its enterprise-wide use cases. Octopus works with existing identity infrastructure without costly redesign. IT leaders ensure high-assurance, phishing-resistant login across all IT-managed apps and services anywhere at any time.

Aite Novarica **Get Report**

The Business Case for Octopus Passwordless MFA

Zero-trust Identity Pays Quantifiable dividends

Passwordless MFA slashes the attack surface and helps, helps workers and IT admin be more productive while implementing a high-assurance authentication program that pays business dividends.

[Calculate your own ROI]

ROI

8x
Worker and IT admin productivity gains

35x
Security risk buy down

Octopus Delivers the Best Enterprises Results

Enterprises seeking passwordless solutions must consider key factors, including security, ease of implementation, interoperability, and cost-effectiveness.

	Security	Ease of implementation	Interoperability
Octopus	**Enterprise-wide passwordless:** Users never create, remember, type or expose passwords.	**No upfront redesign of apps or directories:** Enterprise-wide coverage in weeks/months.	Compatible with SSO, FIDO and password apps out of the box and works with heterogenous vendor directories.
Others Password-less	**Less frequently used passwords:** Users set, use, and reset their directory passwords.	**Redesign apps and directories for vendor's SSO IDP:** Enterprise-wide coverage in months, years, or not possible.	Only compatible with Windows and SSO.

Meet Security and UX Goals in a Fraction of the Time and Cost

Other offerings require costly upgrading all of your apps and directories to the vendor's requirements before eliminating user passwords. By working with existing apps and infrastructure, Octopus delivers the benefits of passwordless without recoding first so you can modernize backend apps and infrastructure at IT's own pace — and in a fraction of the time.

Extend Your IAM Investments to Enterprise-wide Passwordless

IAM vendor solutions deliver partial enterprise passwordless use case coverage leaving your business exposed to security risks and limiting the passwordless ROI your business realizes. Octopus extends IAM vendor investments to cover every app and service your business and workers relies on.

	Passwordless		
	SSO	Non-SSO	Users never know or use passwords
Microsoft Entra ID, okta, PingIdentity	Yes	No	No
+	Yes	Yes	Yes

How IT Works

The Octopus Authentication Platform is built around a patented technology called Invisible Secret Rotation. The platform replaces the user's directory password entry with a machine-generated token that the Octopus manages and rotates. The user never knows that token exists or when it is rotated. Instead, users authenticate to Octopus using stronger passwordless methods like FIDO2, passkey, smartcards, OTP tokens, and mobile push. Once the user has passed the high assurance authentication, the Octopus orchestrates access to user desktops, SSO, remote services, and password-based apps without passwords.

Ephemeral and Entropic Tokens

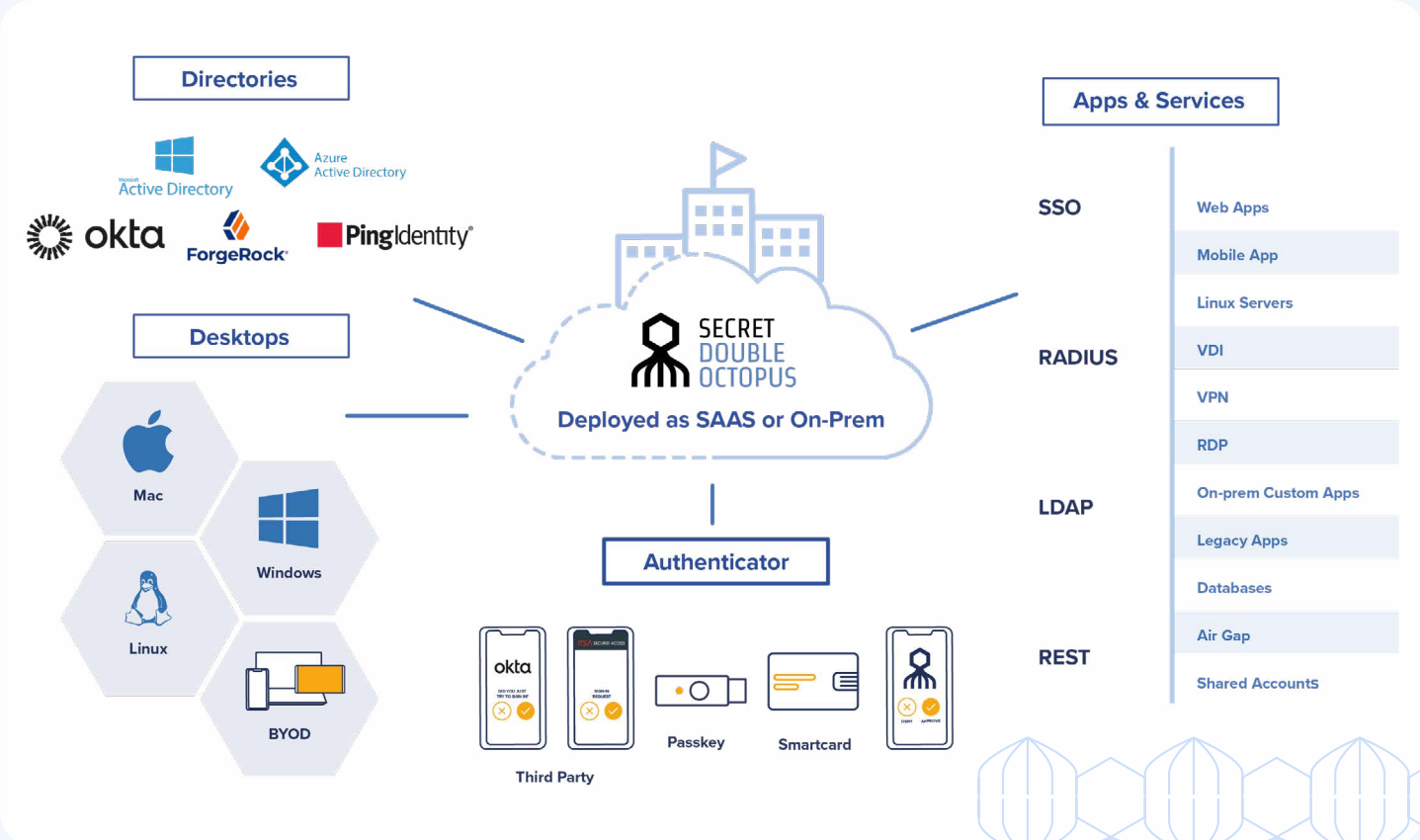
The Octopus tokens rotate at regular predefined intervals of minutes, hours, days, or weeks, and on-demand by the administrator. Since the user never knows or types the token, it can be complex, up to 64 random characters. However, because of the random nature of the token's value, even short eight-character tokens are difficult to hack and too short-lived to be of value to an attacker.

SaaS Deployment, On-prem, and Air Gap Deployments

Deploy the Octopus Authentication Platform as self-managed appliances on-prem and air gap islands or as a SaaS via the Octopus Cloud. Alternate between on-prem and cloud where high availability is needed to support your business strategy.

Fallback and Recovery

Fast recovery from broken, lost, or unavailable user authenticators is an essential capability for passwordless technologies. Other passwordless methods that solely depend on FIDO and X.509 certificates have no recovery model, so they leave user password login available as the fallback mechanism, a dangerous practice. With Octopus, when a legitimate user can't access their approved authenticator, IT can send the user a temporary token valid for a short time without changing any other element in the infrastructure or compromising security. Octopus also gives users a self-service portal to add or remove authenticators.



Flexibility to Power Your Unique Passwordless Journeys

Why settle for a one size fits all passwordless solution? Customize your journey to passwordless with your specific needs in mind. Secret Double Octopus offers one unified platform that can leverage third-party MFA authenticators or its own — the most flexible options available today for a passwordless journey.

With Double Octopus flexibility, organizations can uniquely:

Go passwordless when you are ready, using the same backend components for both MFA or passwordless deployments.

Mix and match traditional MFA with adaptive push MFA or add FIDO2 hardware keys selectively for different user group workflows, such as admins, production or support personnel.

Use Octopus Pro to integrate into most third-party authenticators for a wide variety of use cases

Roll out passwordless progressively, starting with our unique "Password Free" mode of operation that allows end users to still set a shared secret but get accustomed to using SDO's authenticator by never having to remember or type it in.

Octopus Platform Editions Comparision

Plan Features	Starter	Pro	Enterprise
Octopus Authenticator	X	X	X
MFA for Web and Mobile Apps	X	X	X
MFA for VPN & VDI	X	X	X
SSO Portal (Optional)	X	X	X
SSO Portal Passkey Support (Cloud Sync'd)	X	X	X
FIDO Security Key Support (Device Passkeys)	X	X	X
Phishing-Resistant MFA	X	X	X
Desktop MFA (PW-based)		X	X
Desktop Push Bombing Protection		X	X
3rd Party Authenticator Support		X	X
OTP Authentication Fallback		X	X
AAL3 Proximity Assurance		X	X
Desktop-to-App Pinning		X	X
Mac Local FileVault Supported		X	X
Smartcard Desktop Authentication			X
Desktop MFA (Passwordless)			X
Secure Shared Accounts			X
Legacy Apps (domain joined)			X
Legacy Apps (stand alone, DB identity)			X
Desktop SSO (for password apps)			X

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**.

SECRET DOUBLE OCTOPUS

Learn more at **doubleoctopus.com**