

Passwordless for the Working Enterprise

REQUEST A DEMO

SOLUTION OVERVIEW



Table of Content

Solution Overview	3	Built for the Working Enterprise	12
Rethinking Work Force Authentication	4	Extend Existing On-Prem Directory Service.....	13
Addressing Enterprise Authentication Challenges.....	4	Offline Authentication	13
Passwordless Authentication.....	5	No Phone	14
Passwordless Enterprise.....	6	A Choice of Authenticators	14
Next Generation MFA.....	7	How It Works?.....	15
Why Secret Double Octopus?	8	Go Passwordless With the Octopus Authenticator.....	15
Gradual Migration to Passwordless Authentication	9	Go Passwordless With FIDO	16
Unified Experience	10	Passwordless Access for Desktops	17
Exceptional User Experience	10	Ready to Meet the Octopus?.....	18
High-Assurance Authentication.....	11		
Reduced Operational Costs	11		

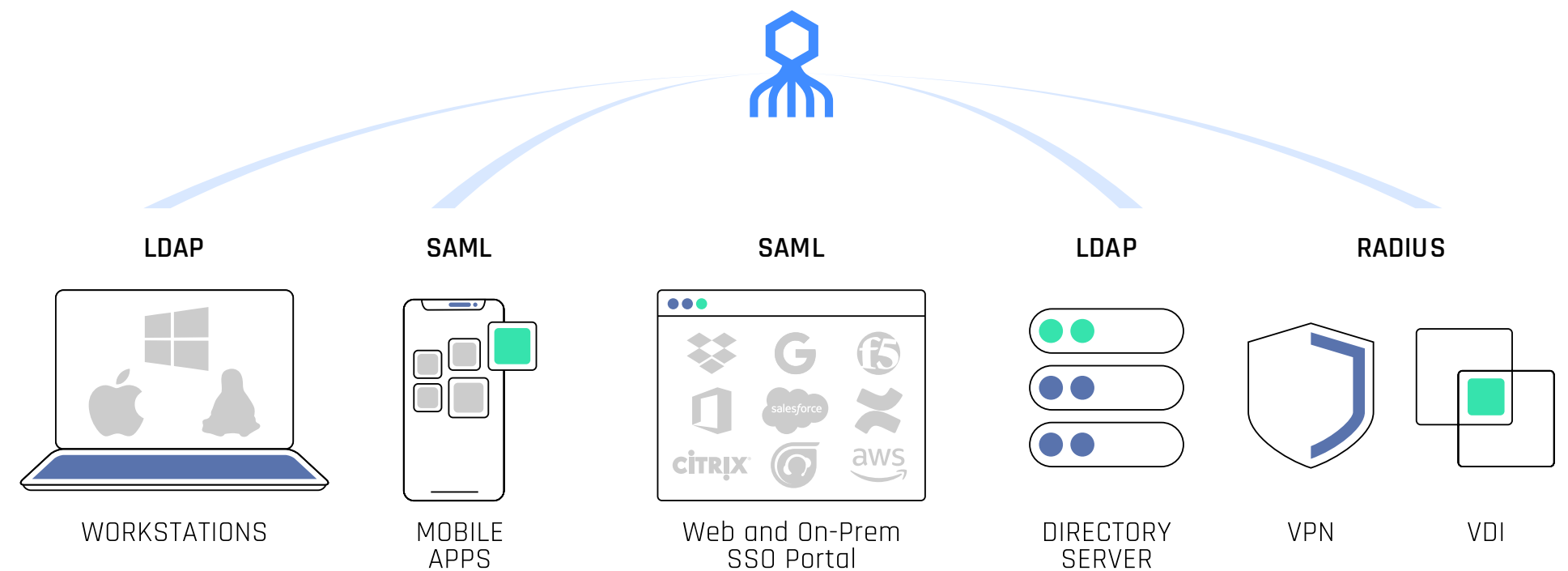
Solution Overview

Octopus Authentication is a high-assurance, passwordless authentication system engineered to address the diverse authentication needs of a real-world, working enterprise.

For users, it offers a **simple “touch-and-go” experience to access all enterprise resources** whether on-premise or in the cloud, online and offline. It requires no passwords to key-in and supports a broad range of mobile and FIDO-compliant authenticators.

For IT admins, it offers **an authentication solution that is cost effective to operate** and supports both modern and legacy infrastructure and applications, deployed on-premise or in the cloud.

As a result, Octopus Authentication can be ubiquitously deployed across all business systems and applications to support all authentication use-cases. And for enterprises that are not ready to go full passwordless from day one, Octopus Authentication offers a gradual migration path to eliminating the password.



“I would surely recommend Secret Double Octopus to our partners for their substantial advantages compared to other vendors in terms of security and efficiency for the organization.”

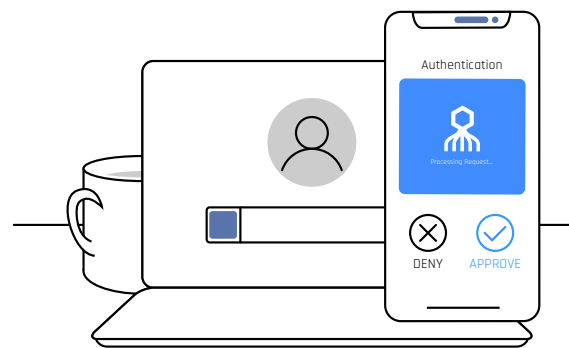
T-Mobile

Yosef (Seffi) Yaaran | Principal Architect
PaaS/User experience at T-Mobile

Rethinking Work Force Authentication

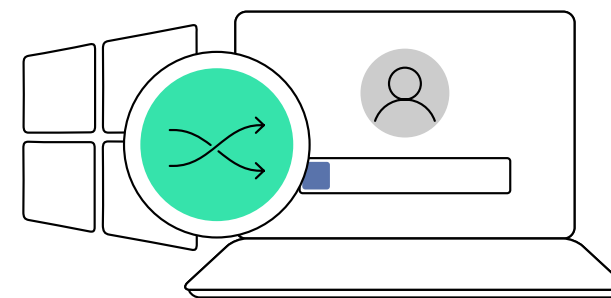
Addressing Enterprise Authentication Challenges

Octopus Authentication addresses three common authentication challenges experienced by enterprises operating a heterogeneous IT environment.



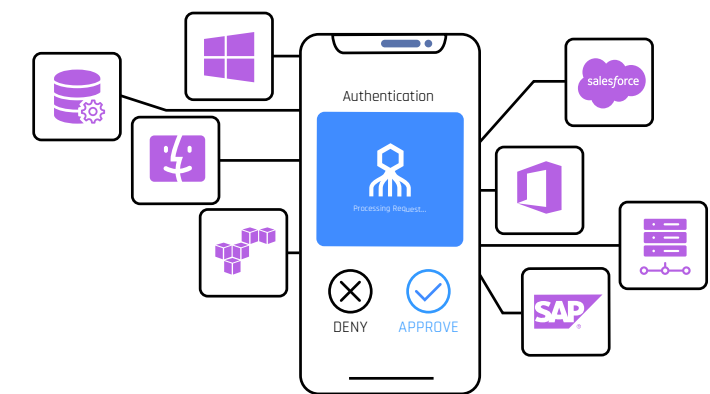
PASSWORDLESS AUTHENTICATION

Allowing businesses to improve their security posture by getting rid of vulnerable passwords, and replacing them with a high-assurance passwordless authenticator.



PASSWORDLESS ENTERPRISE

Replacing static, user-controlled passwords with frequently updated, machine-generated passwords, to improve the security posture of systems and applications that require passwords.



NEXT GENERATION MFA

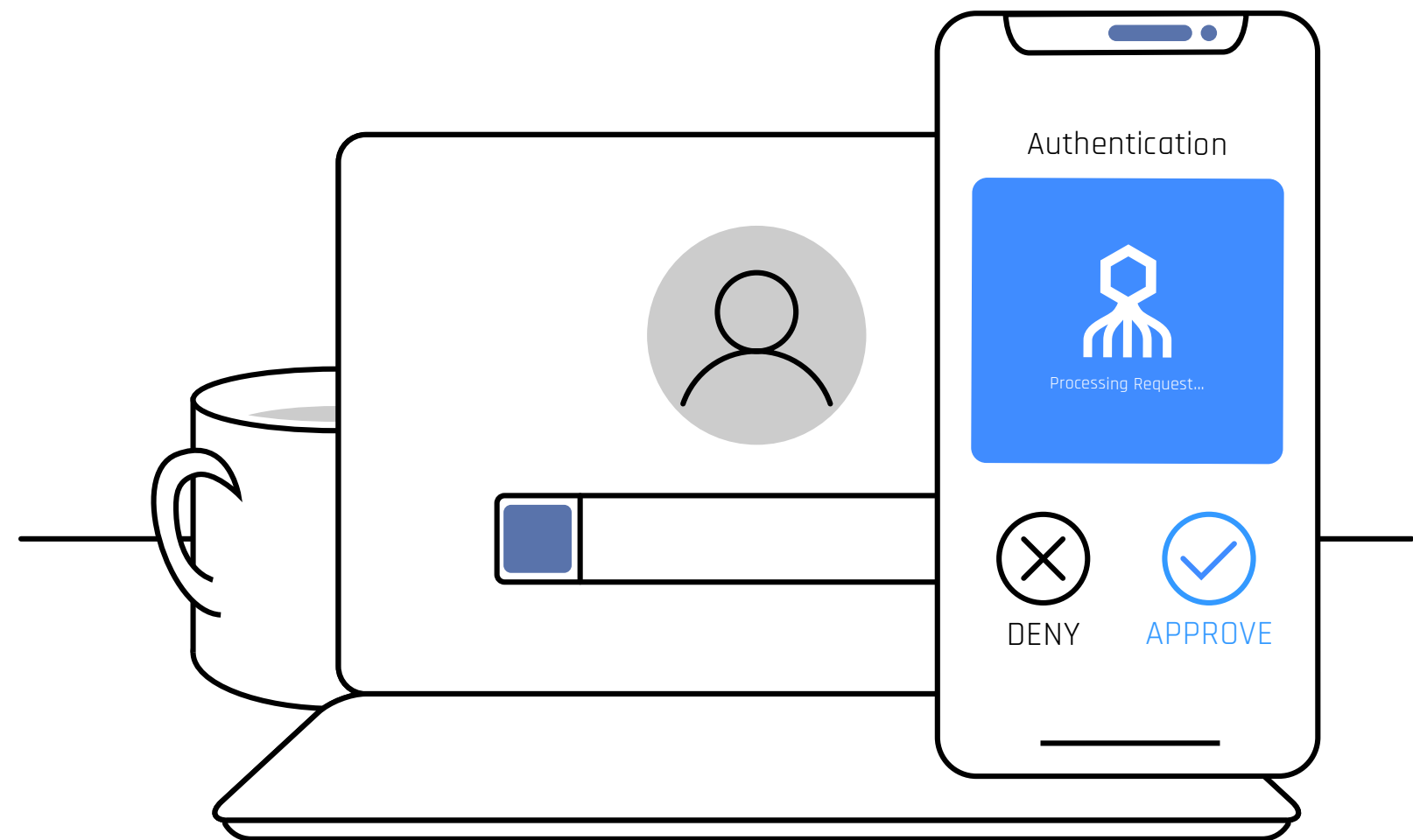
Passwordless or password-based multi-factor authentication that can be deployed across all workstations and businesses system, including those that were not designed with MFA in mind.

■ Passwordless Authentication

Passwordless authentication allows businesses to eliminate vulnerable passwords which are frequently used to gain unauthorized access to business systems and applications. In addition to improving security posture, the removal of passwords increases user productivity, and significantly reduces password management and support costs.

Secret Double Octopus helps businesses replace passwords with a passwordless authenticator. Instead of entering a password, users simply approve an authentication request securely delivered to their Octopus Authenticator app, or use their FIDO2-compliant authenticator. Users never have to create, recall or change another password.

Secret Double Octopus supports a heterogeneous authentication environment with a broad range of passwordless authentication options, including FIDO-compliant authenticators.

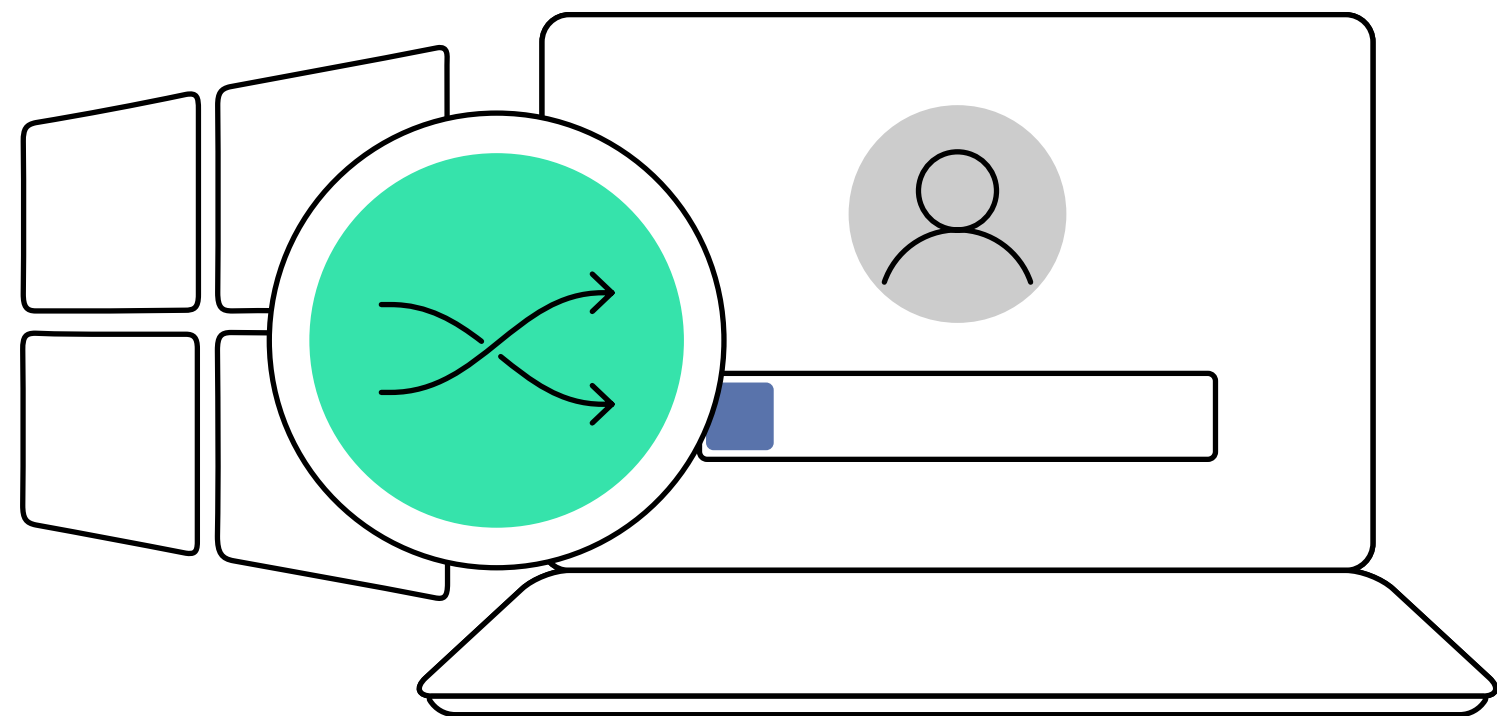


■ Passwordless Enterprise

While achieving a passwordless workplace is a goal for many businesses, reality often makes it difficult to break free from passwords. Many enterprise customers still rely on passwords to make their business run. Typically, older systems and applications are still dependent on passwords for authenticating users and are not yet optimized to support passwordless authentication.

Octopus Authentication replaces static user-controlled passwords with machine-generated passwords which are controlled by the company and not its employees. Instead of recalling and entering passwords, users simply authenticate using the Octopus Authenticator on their mobile device. Following successful authentication, the Octopus Authentication Server generates a long, complex session password that is securely delivered to the relying system. A fresh password will be generated for every session without the user involvement.

As a result, businesses can deploy **high-assurance, passwordless authentication** for legacy systems that depend on passwords, and users benefit from a passwordless experience.



Next Generation MFA

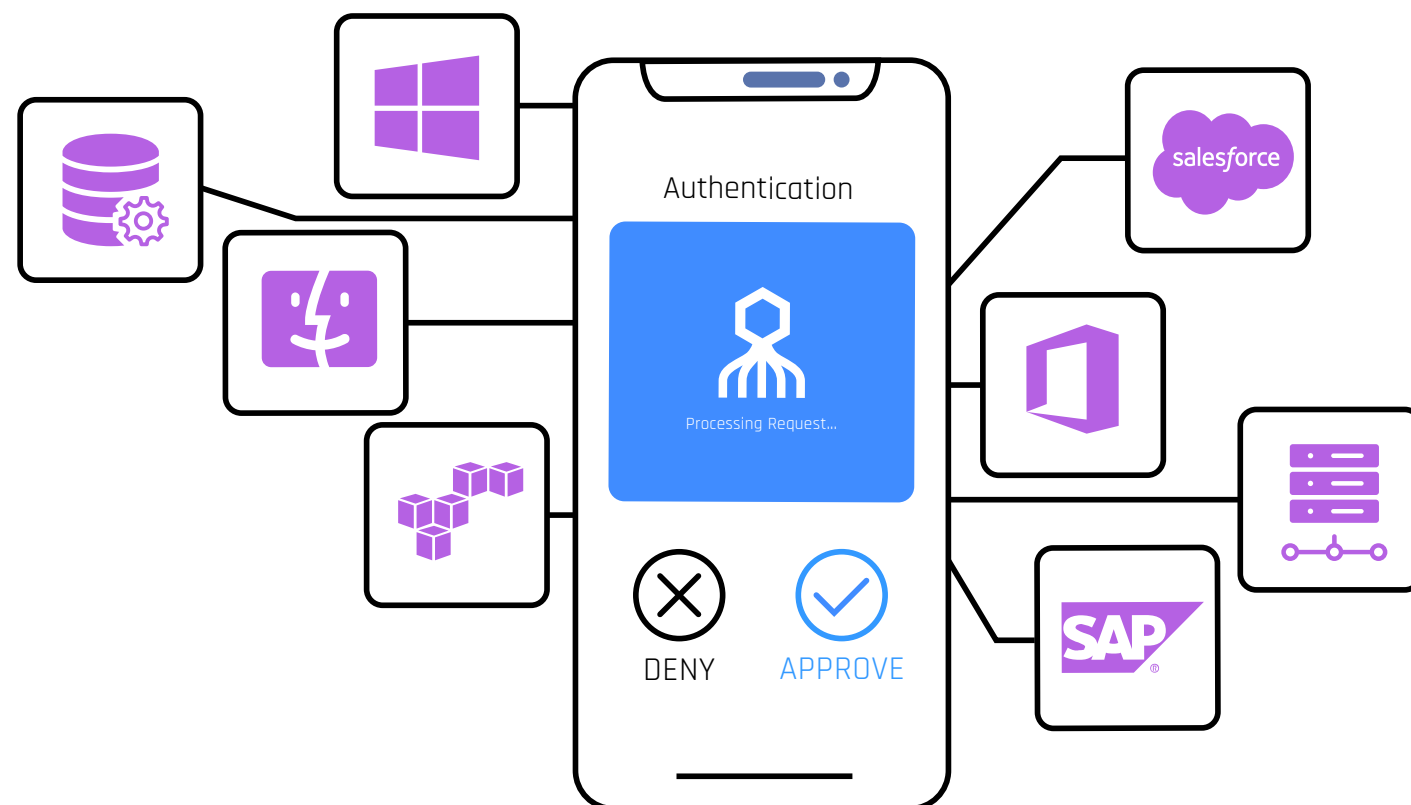
Deploying multi-factor authentication (MFA) is often hard from a technical and a user acceptance perspective. Technically, MFA projects typically come up against older systems that do not support the interfaces required to work with an MFA Solution. Passwordless MFA is even harder to deploy, because many systems still rely on passwords to authenticate users. When it comes to users, they hate elaborate MFA solutions that are a hassle to operate.

As a result, typical MFA deployments cover only remote access VPN and cloud access.

Octopus Authentication delivers a hassle-free MFA solution that protects EVERY login, on both legacy and modern systems.

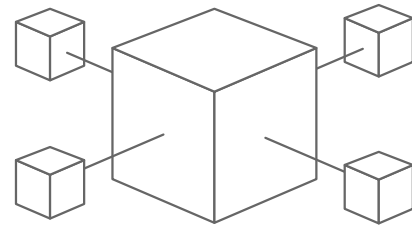
Passwordless MFA from Secret Double Octopus uses cryptographically secure out-of-band push notifications to the user's mobile device to ensure only the authorized user in possession of their

registered device can successfully authenticate. Layering biometric authentication to access the Authenticator results in passwordless multi-factor authentication that is easy to use and highly resistant to credential theft and man-in-the-middle attacks.

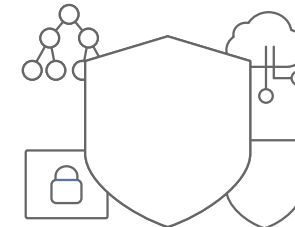


Octopus Authentication delivers a **hassle-free MFA solution that protects EVERY login**, on both legacy and modern systems.

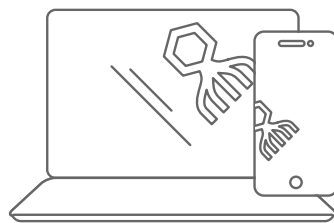
Why Secret Double Octopus?



**GRADUAL MIGRATION
TO PASSWORDLESS
AUTHENTICATION**



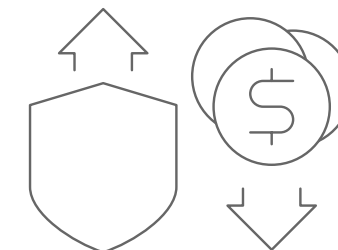
**UNIFIED
EXPERIENCE**



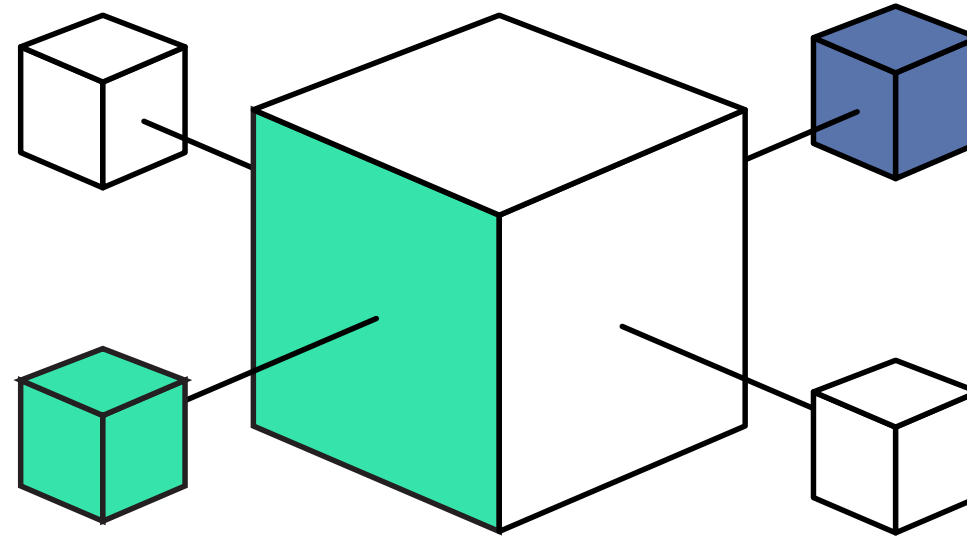
**EXCEPTIONAL USER
EXPERIENCE**



**HIGH-ASSURANCE
AUTHENTICATION**



**LOWER
OPERATIONAL COSTS**

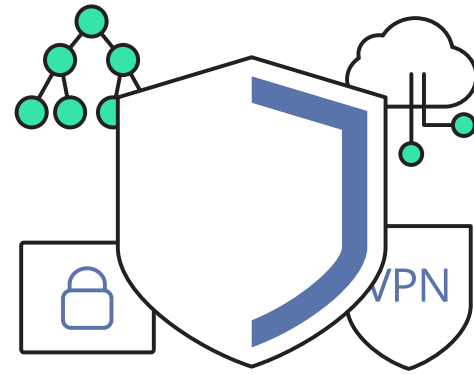


Gradual Migration to Passwordless Authentication

It is widely acknowledged by industry, regulatory and security experts that passwords are vulnerable, expensive to manage and negatively impact user experience and productivity. Therefore many enterprises have set their sights on moving to passwordless authentication. But migration to passwordless often proves challenging to execute, given the many legacy systems and applications which do not support the technology.

Secret Double Octopus enables enterprises to operate heterogeneous authentication technologies and manage a gradual introduction of

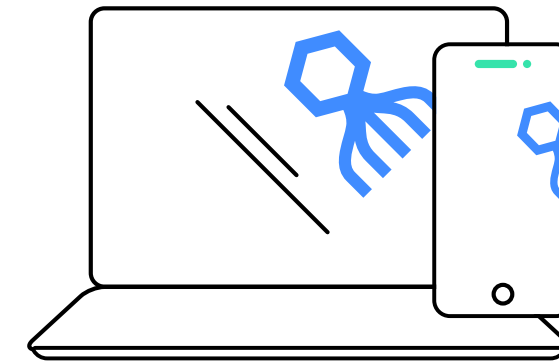
passwordless authentication. Once a system is configured to work with the Octopus Authentication Server, switching users to passwordless requires a simple toggle of a switch. Typical deployments include rolling out a passwordless solution to a subset of the workforce, and gradually expanding to the entire workforce, or going passwordless on a subset of systems, and gradually adding more systems until a password-free workplace is achieved. Once users are migrated to Octopus Authentication, legacy authentication technologies can be retired.



Unified Experience

Deploying add-on solutions to address authentication gaps for specific use-cases or systems means putting more authentication credentials in the hands of users, and creating more opportunities for them to call on the help desk for help. Users want one simple way to access all of their applications.

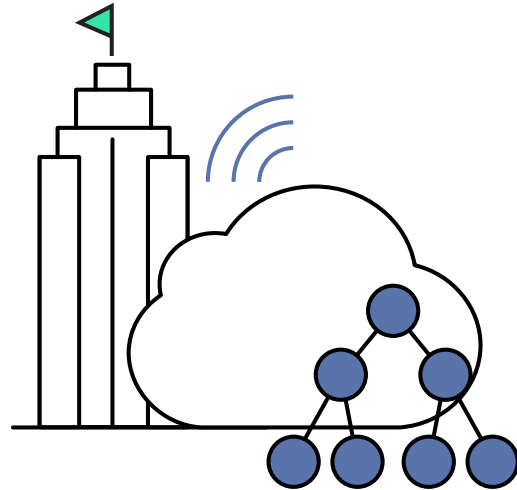
Secret Double Octopus delivers an authentication solution that works across all business systems and applications, and in concert with existing authentication solutions, to provide users with one authenticator that will let them access all of their applications. Octopus Authentication will broker all authentication requests to enable a unified experience for users, while working in the backend to negotiate authentication with third-party systems.



Exceptional User Experience

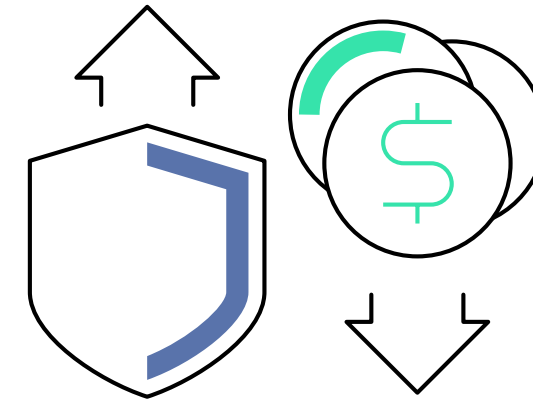
The Octopus Authenticator offers a simple “touch-and-go” experience to access all enterprise resources whether on-premise or in the cloud, online and offline, for end users and also privileged admins. There are no passwords to key in and no hardware authenticators to fiddle with.

Users authenticating with FIDO2 authenticators, typically to web applications (via web browsers), can use their FIDO authenticator to access all other systems and applications that work with Octopus Authentication, including their workstations, remote access VPN, single sign-on, and more.



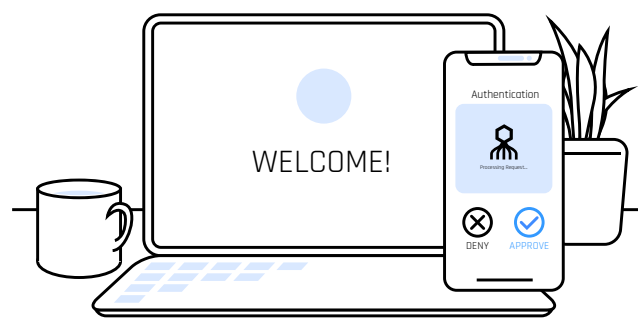
High-Assurance Authentication

Octopus Authentication utilizes provably unbreakable cryptography that is quantum-safe and highly resistant to common attacks such as phishing, MITM and password cracking. When used to authenticate to legacy systems that require passwords, Octopus Authentication replaces static user-controlled passwords with machine-generated passwords that are controlled by the Octopus Authentication System.



Reduced Operational Costs

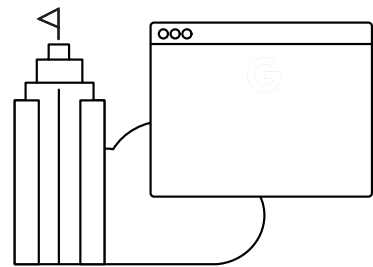
Delivering a passwordless experience means quicker logins and less downtime for users, and lowers workloads for helpdesks. It also eliminates password management costs and frees up the phishing-prevention budget.



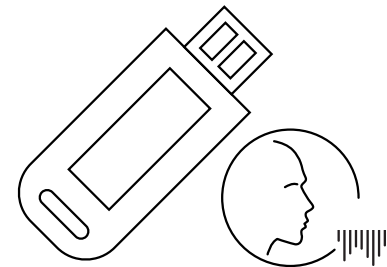
With 25% to 40% of all help desk calls attributed to password problems or resets, and the immeasurable employee downtime resulting from slow logins or inability to login because of forgotten passwords or lost authenticators, deploying a hassle-free authentication solution quickly pays for itself.

Built for the Working Enterprise

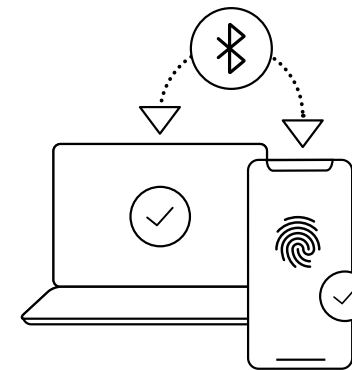
Octopus Authentication is engineered to address the needs of real-world, working businesses. It is therefore equipped with all the facilities needed to support heterogeneous IT environments comprising modern and legacy systems, deployed on premise or in the cloud.



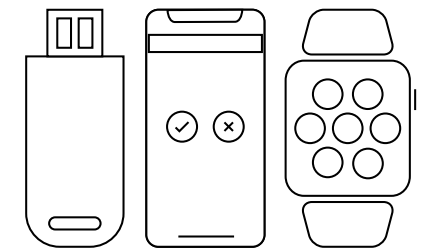
**EXTEND EXISTING
ON-PREM
DIRECTORY SERVICE**



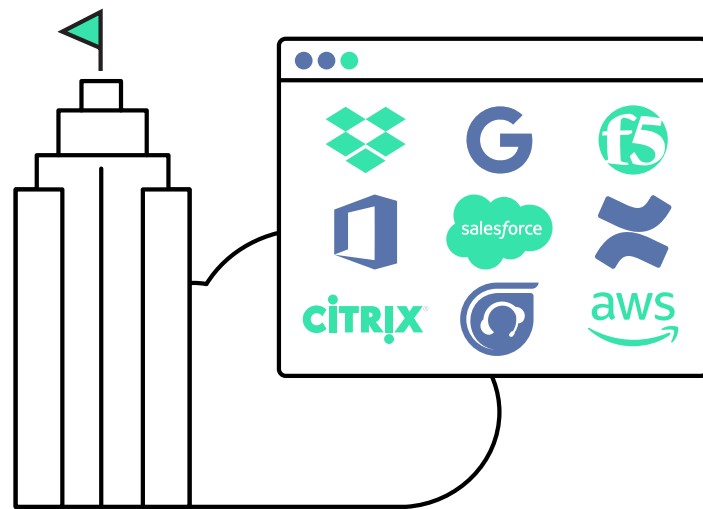
NO PHONE



**OFFLINE
AUTHENTICATION**

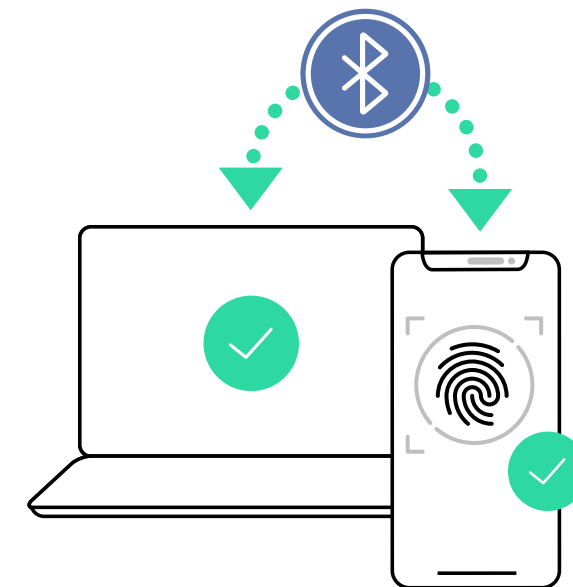


**A CHOICE OF
AUTHENTICATORS**



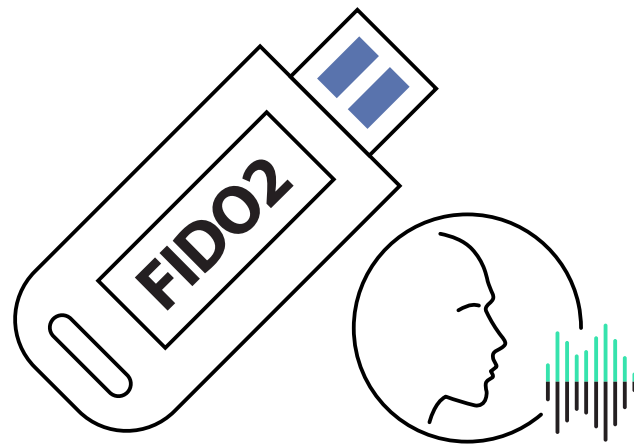
Extend Existing On-Prem Directory Service

Octopus Authentication equips an existing LDAP directory used for authenticating users to the company domain with an interface to authenticate users to cloud applications. Employees can authenticate to any cloud service that supports web authentication standards such as SAML and OpenID Connect (OIDC).



Offline Authentication

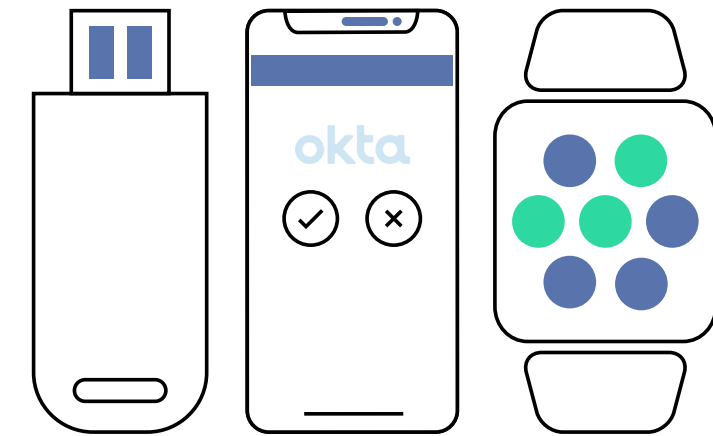
To ensure passwordless authentication does not limit employees, Octopus Authentication supports workstation logon even when there is no connectivity to the authentication server. Using a local wireless connection between the phone and the workstation (BLE - Bluetooth Low Energy), users enjoy the same authentication experience even when offline.



No Phone

Octopus Authentication supports any FIDO2-compliant authenticator, so in those increasingly rare situations where users don't have a smartphone on which to install the Octopus Authenticator app, or simply do not want a company app on their personal device, Octopus Authentication supports alternative authenticators. Supported authenticators include hardware tokens such as Yubikey and voice authentication.

In the case of a lost or forgotten authenticator, Octopus Authentication generates a temporary credential to prevent employee downtime.



A Choice of Authenticators

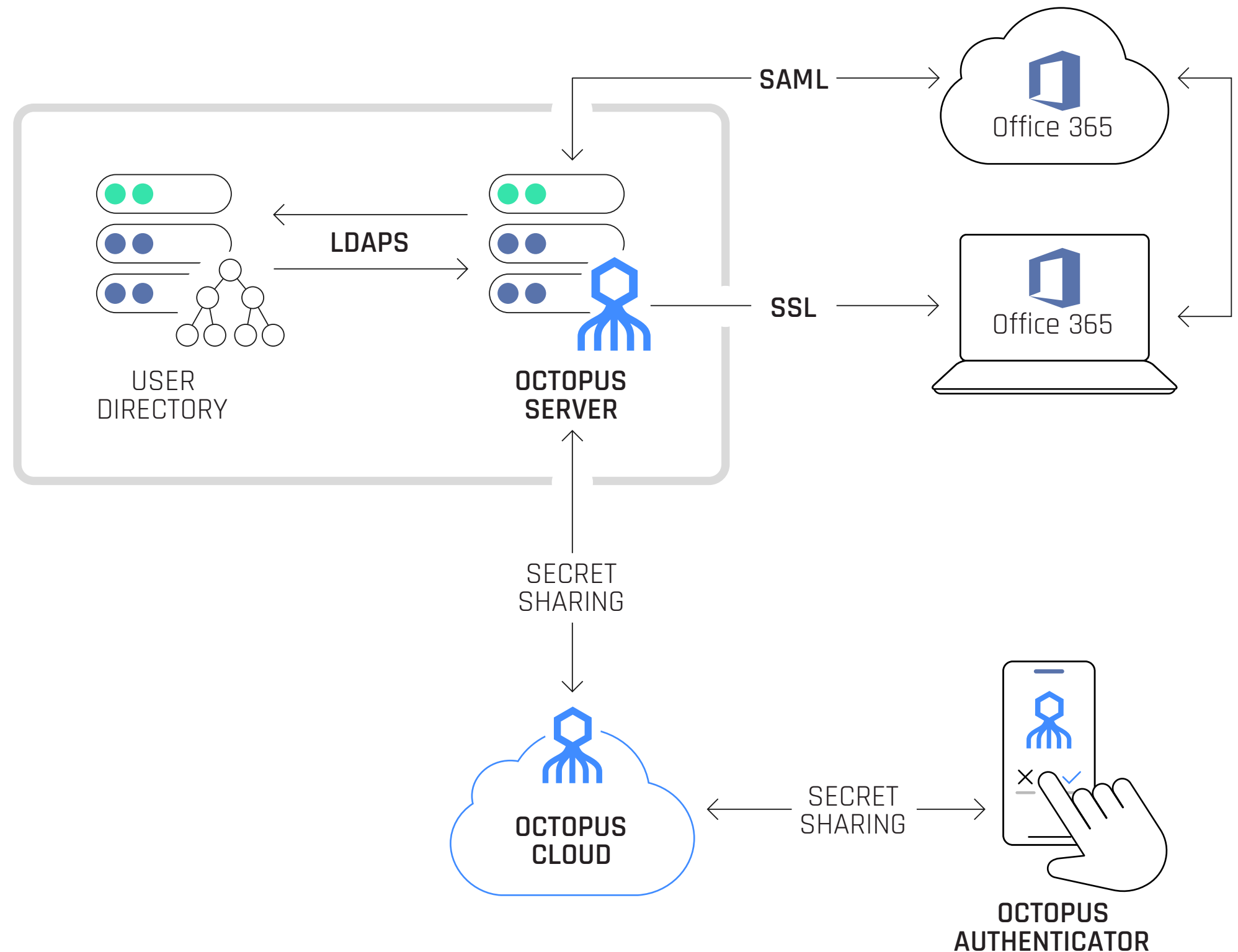
The Octopus Authentication Server is FIDO2 compliant, which means it supports the Octopus Authenticator and also any other FIDO2-compliant authenticator. Businesses can therefore choose the authenticator they prefer, or use a mix of authenticators.

Octopus Authentication also supports deployment options that allow it to work in concert with any existing authentication solution. There is no need to rip-and-replace existing authentication solutions. Octopus Authentication is able to orchestrate multiple third-party authentication solutions, and when the time is right, enable the gradual retirement of legacy authentication solutions and replace them with Octopus Authentication.

How It Works?

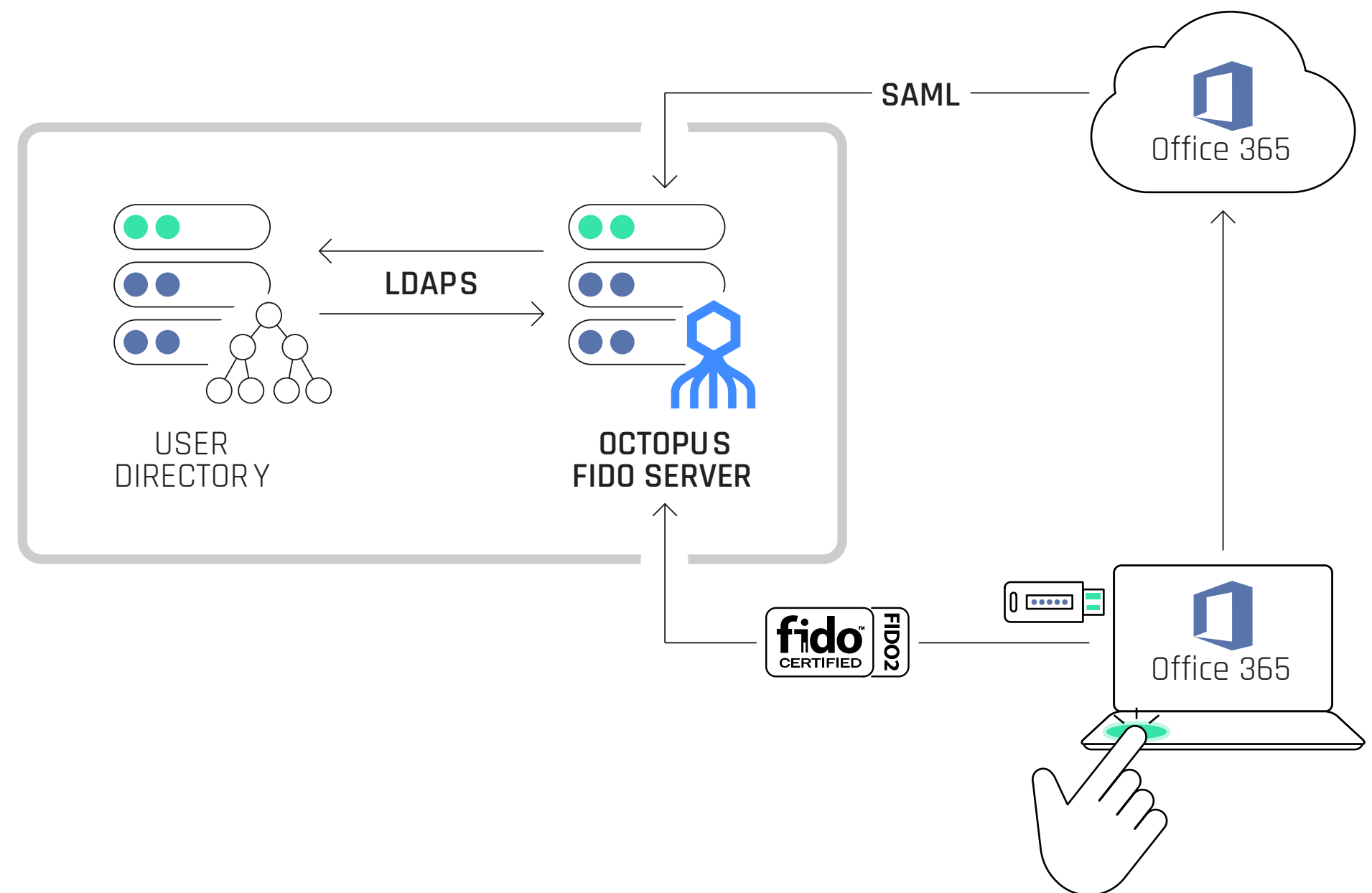
Go Passwordless With the Octopus Authenticator

Secret Double Octopus replaces passwords with a high-assurance passwordless authenticator. Users requesting to logon to their workstation, authenticate their VPN connection or sign into an application receive a secure push notification to the Octopus Authenticator app on their mobile device. Push notifications are securely delivered via the Octopus Cloud Service using Secret Double Octopus's unique secret sharing technology. Once the authentication request is received in the Octopus Authenticator, users provide a biometric print for authentication - typically a fingerprint using the sensor built into their mobile device - and tap 'approve' to accept the authentication request. An authentication attestation is then sent from the Octopus Authenticator back through the Octopus Cloud Service to the Octopus Authentication Server, and then to the relying system. Upon receiving the response from the Octopus Authentication Server the relying system grants access to the user.



Go Passwordless With FIDO

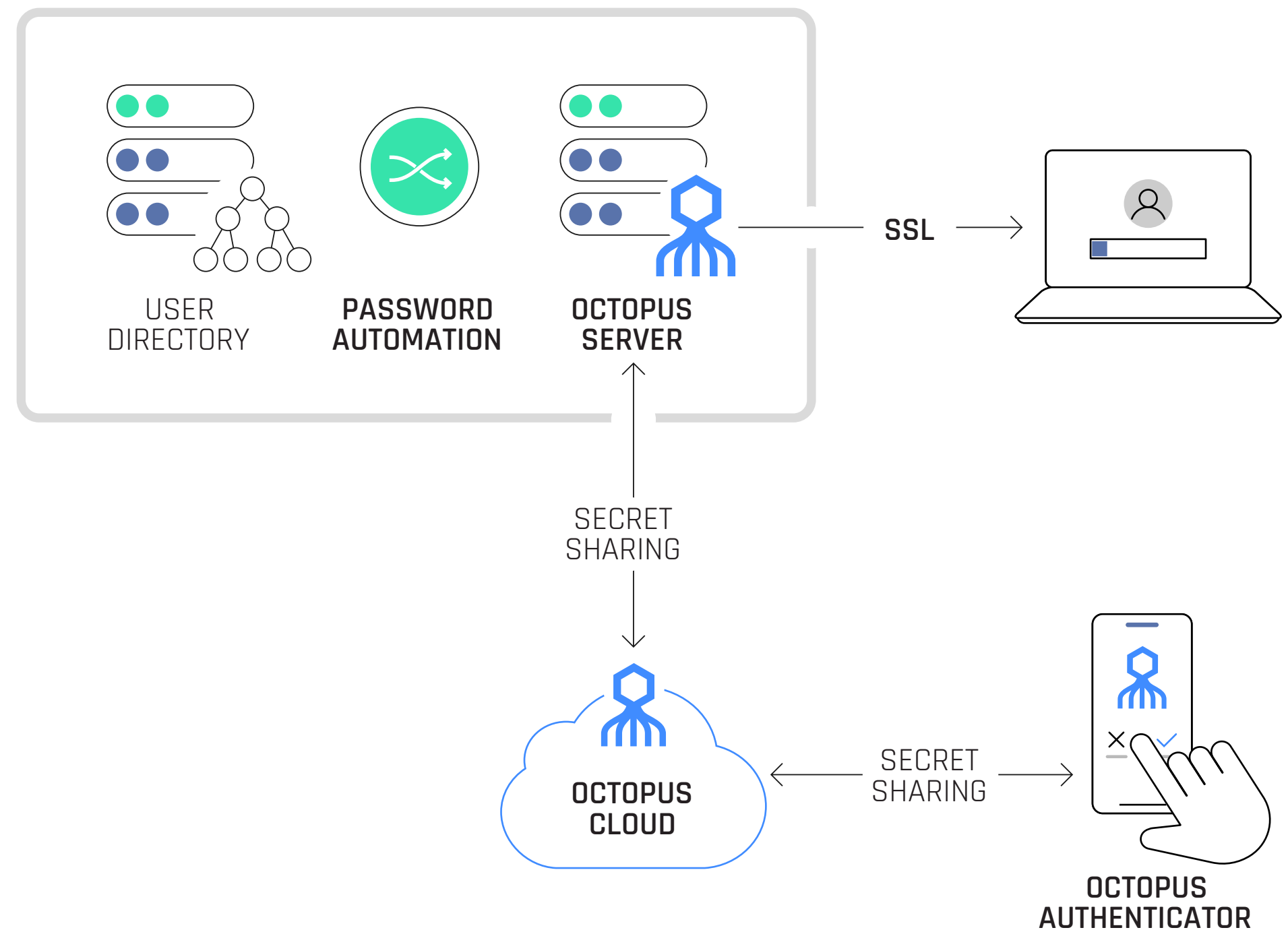
Secret Double Octopus supports passwordless authentication using FIDO-compliant authenticators. To logon to their workstation, users simply plug-in their FIDO authenticator to the workstation's USB port. A challenge generated by the FIDO Server is relayed to the FIDO Authenticator via the Octopus Credential Provider on the workstation. The user approves the challenge request - typically by tapping the authenticator or providing a fingerprint. The FIDO Authenticator's response to the challenge is then relayed via the Octopus Credential Provider to the FIDO Server, which in turn responds to the relying system with an authentication approve/reject. Authentication to web-based applications is performed using native browser support for WebAuthn.



Passwordless Access for Desktops

Secret Double Octopus enables passwordless workstation logon using its Octopus Credential Provider. To access their workstations, Windows or Mac users simply enter their username in the Octopus Credential Provider running on their workstation. The Credential Provider communicates with the Octopus Authentication Server, which looks up the user and sends a secure push notification to the Octopus Authenticator app on the user's registered device. The user in turn authenticates to the Octopus Authenticator app and approves the authentication request. The Octopus Authentication Server then communicates with the Domain Controller to complete the logon process.

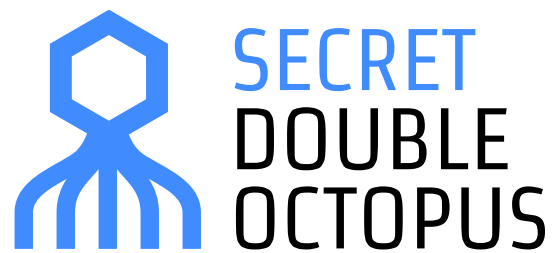
To enable users to logon to their workstations even when offline, the Octopus Authenticator communicates with the Octopus Credential Provider directly over a local BLE connection.



Ready to Meet the Octopus?

REQUEST A DEMO

DOWNLOAD OUR
TECHNICAL DATASHEET



contact@doubleoctopus.com

sales@doubleoctopus.com

