SECRET DOUBLE OCTOPUS

SOLUTION BRIEF

Close Security Gaps in Shared Accounts

Industry Problem Statement

No IT security leader likes it to admit it, but shared accounts still exist in many business operations. Though they clearly add risk, shared accounts prove more convenient and often less costly than a “one account, one user” approach.

Faced with industry mandates aimed at securing identity, businesses need to find cost-effective ways to implement multi-factor authentication (MFA) without disrupting shared access workflows.

Solution Statement

The Octopus passwordless MFA platform streamlines individual users’ access to shared workstations and servers with fast and easy passwordless logins. Workers never need to create, remember, write down, or share passwords to access resources and get their jobs done.

Octopus strengthens enterprise security and delights individual users with intuitive authentication workflows that pay the business dividends:

- Slash the attack surface
- Create an audit trail for shared accounts
- Takes about an hour to connect Octopus and start onboarding users

Octopus closes security risks and produces a reliable audit trail for documenting actual user access to shared accounts. The Octopus platform delivers enterprise passwordless MFA that:

- Resists impersonation
- Resists theft
- Resists insider collusion
- Works with on-prem Active Directory (AD)
- No recoding apps or rearchitecting identity infrastructure
- Works with modern and legacy apps and systems

Passwordless MFA strengthens user access in mission-essential shared account workflows:

Factory and production shift worker

Privileged user local and network access

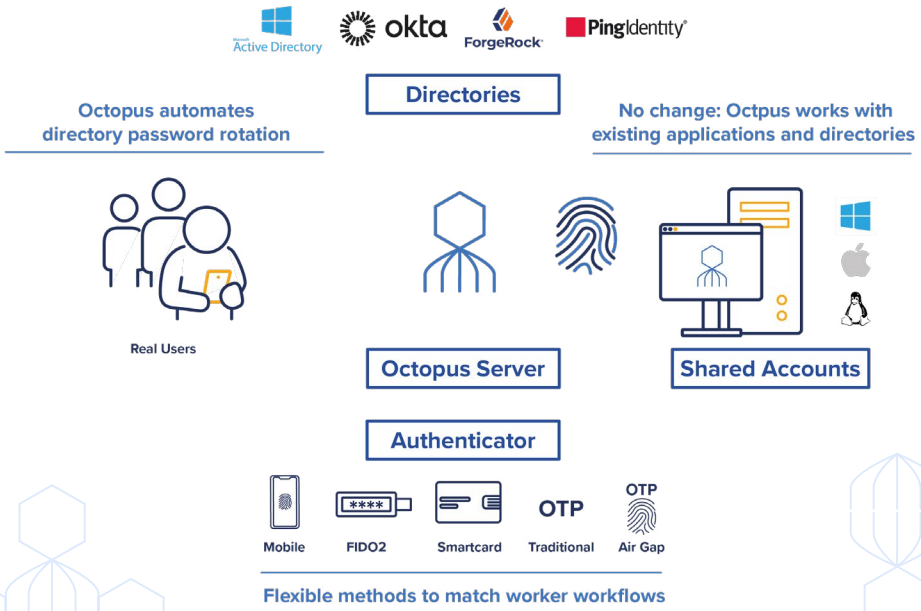
24/7 healthcare station access

Business applications sharing

How it Works

Octopus protects shared workstations, servers, and HMI kiosks with individual users' strong authentication.

IT can manage user and shared accounts in single or multiple federated or unfederated individual directories or as local Octopus users. The platform manages and rotates user and shared account directory passwords within the backend infrastructure.



Benefits

Strong authentication with no shared secrets

Audit trail of users accessing shared accounts

Avoids the expense of recoding applications and re-architecting directories

Summary

Unlike other security technologies that add complexity to gain security, Octopus enables less—less work and less risk with less cost–while delivering more and greater business returns. Slash your attack surface, make your workforce more productive, and spare IT the grueling job of rearchitecting infrastructures to close security gaps.

- Enables phishing-resistant MFA enterprise-wide
- Workforce logins faster with less frustration
- IT moves faster without supporting user-managed secrets

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 more secure and 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**