

**DATA SHEET**

# Extend Windows Hello to Everything

Use Integrated Biometrics to Access Password-Based Apps, Network services & On-Prem Assets


## Windows Hello is a Great Start

Windows Hello for Business (WHfB) gives workers a convenient and secure way to access Windows machines and Entra ID compatible SaaS apps without typing passwords. But for all other resources, users are left frustrated and the business is left exposed to unnecessary password and phishing risks.

## But Leaves Too Many Gaps

Coverage gaps force workers to continue to type their directory passwords to access systems they need throughout their workday. And leave exposed weak links for attackers to exploit:

- On-prem & legacy applications
- Remote access & network services
- Shared accounts
- Fallback when authenticators fail or go missing

- 
- ✓ **Easy login using integrated Windows biometrics**
  - ✓ **Unified user experience across all enterprise use cases**
  - ✓ **ZeroPassword™ technology eliminates all user-managed passwords**
  - ✓ **Works with all password-based apps without a redesign**

# Octopus WHfB Booster

Octopus changes all that. Octopus works with WHfB authentication out of the box and extends passwordless authentication workflows across your entire enterprise, including access to password-based apps and network services.

Octopus is compatible with your existing apps and identity infrastructure. So, you achieve your user experience and security goals in a fraction of the time and at a fraction of the cost.

WHfB only cover the tip of the attack surface and user frustration



Windows Desktop



SSO SaaS



VPN



VDI



RDP



SSH



Self-Managed On-Prem

Custom & Legacy Apps



AD Joined



Stand-alone



Shared Account



Industrial Gap



Mac Desktop  
Unified 100% use case coverage

Octopus extends WHfB to everything in the enterprise

Octopus' patented ZeroPassword™ technology replaces all directory & legacy credentials with machine-generated ephemeral tokens that no one ever knows. So users never create, remember, type, or fall back to passwords anywhere.

Because our token-based approach is compatible with your existing applications and directory infrastructure, no costly redesign is required and enterprise-wide deployment happens fast.

## Benefits



- ✓ **Improve security with phishing-resistant authentication for every access**
- ✓ **Make workers 5% more productive every day**
- ✓ **Avoid password frustration and MFA fatigue**
- ✓ **Lower IT operating costs – no password management overhead or added MFA cost**
- ✓ **Comply with zero-trust identity security requirements ahead of audits**

## About Us

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 at scale.

Our platform integrates seamlessly into any infrastructure, supporting any system, use case, or authentication method. Trusted by SMBs and Fortune 50 enterprises alike, we secure over a billion authentications annually, enabling organizations to achieve modern, phishing resistant security.

**Let's redefine authentication.**

Learn more at [doubleoctopus.com](https://doubleoctopus.com)

© Copyright Secret Double Octopus, Ltd All Right Reserved. All trademarks herein are trademarks of their respective owners.

