SECRET DOUBLE OCTOPUS

CASE STUDY

Multi-national Defense Manufacturer Adopts Unified Passwordless MFA

Upleveling User Authentication and IT Agility

Octopus Authenticator Streamlines Onboarding Across Diverse Business Groups

Overview

A major defense manufacturer sought a passwordless MFA solution to protect sensitive data, improve its end-user authentication experience, and lower help desk password reset costs. The company selected the Octopus Authenticator Platform to roll out a unified passwordless UX across autonomous business units worldwide.

Customer

Industry: Defense manufacturing

Location: Multiple sites worldwide

Size: Several thousands per site

Challenge

Move to passwordless MFA that improves the user experience (UX), seamlessly integrates with Active Directory (AD), and supports a broad range of workforce applications and endpoints including Windows and Mac

Solution

Octopus Authentication Platform, Enterprise Edition

Results

Unified passwordless MFA solution across business groups worldwide

- Easy onboarding
- Improved user experience
- Reduced Help Desk password resets

Challenge

The manufacturer initially implemented time-based OTP (TOTP) and smart cards to protect the company's intellectual property and sensitive customer data. Despite having multiple authentication technologies available, the core IT identity management team believed a passwordless MFA solution would improve user authentication, streamline onboarding, and reduce help desk password reset costs but faced trepidation from segregated IT groups concerned about the change required to go passwordless.

Requirements

For the central Identity team sponsoring the idea of standardizing on a passwordless solution, key requirements included:

- **Passwordless authentication—**The Identity team wanted the enhanced security of a passwordless solution despite having to discard incumbent providers that lacked a clear offering
- **Better UX / seamless access—**The group prioritized the user experience over what was best or easiest for IT because, "It doesn't mean much if we can't get users to onboard with the solution"
- **AD integration and lifecycle management—** The new solution needed to interoperate and possibly leverage onboarding, password management, and deprovisioning processes established around Active Directory
- **A secure end-to-end architecture—**The team rejected competing approaches such as setting up key servers in the DMZ that it considered less secure

Solution

After a thorough evaluation of many traditional MFA and other passwordless MFA vendors, the team chose the Enterprise Edition of SDO's Octopus Authenticator Platform. The solution features Password Rotation, an alternative to a PKI certificate-based approach.

"From the moment of receiving a brand-new computer to becoming active, I have never worked with an IAM solution that was as seamless and automatic to onboard."

Results

Over time, SDO's ease of use helped the manufacturer's sponsoring identity team convince all business units to standardize on the Octopus platform. The team reported that, "As soon as people got their hands on it and experienced, concerns with passwordless went away." Ultimately, the benefits of deploying Secret Double Octopus to enhance its strong authentication technologies allowed the company to standardize on passwordless authentication across autonomous businesses.

A trusted partnership for the future

The company plans to continue deploying Octopus Enterprise across all of its commercial businesses and more than 100K employees.

"Hands down, the first priority has to be security, and it's really nice to have a great user experience as well. With SDO we could push both without a lot of complexity on the IT side and check the boxes better than we could with other products."

Why SDO?

The championing team concluded that, despite supporting a password-centric approach, Octopus delivered the full promise of passwordless: end-users never having to create or remember passwords. SDO solved the "last mile" problem of passwordless, as well as the corner use case of legacy on-premises applications that could not be updated via SAML to federation.

Another key difference was that IT could control the password complexity as needed without inconveniencing the user or having to recode applications or rearchitect existing identity infrastructure. Compelling advantages of the Octopus platform included:

- SDO's strong security architecture including the Secret Sharing employed in pushing passwords to a mobile device
- Stronger offline desktop MFA support via Bluetooth
- SDO's "agility compared to larger partners" and the simplicity of onboarding and enrolling users unassisted (for VPN and desktop MFA), a huge plus amidst enhanced remote work scenarios during the pandemic

The team set up some stations to let users try it out and, once they experienced the ease and simplicity, skepticism faded away. Similarly, initial concerns about SDO's ability to support a massive global rollout were laid to rest by the company's innovation, responsive support, and passion for the product.

Learn more at **doubleoctopus.com**

SECRET DOUBLE OCTOPUS