SECRET DOUBLE OCTOPUS

standard chartered

CASE STUDY

Company-Wide Desktop MFA as a Stepping Stone to Full Passwordless

Challenge

Implementing desktop MFA (password-based) across every bank end user for better security and improved user experience, while meeting complex enterprise requirements.

Customer

Industry: Financial Services

Services: Consumer retail banking, trading, investment banking

Headquartered: Singapore

Size: 90,000 employees in over 59 countries

Requirements

- Enable a roadmap with an end goal of “passwordless authentication”
- Support for Windows and Mac endpoint MFA
- Integration with ForgeRock
- Access Manager and Oracle Unified Directory
- Support for non-phone authentication

Results

Octopus Authentication Platform

Today: Octopus Pro (Desktop MFA)

Future: Octopus Enterprise (Full Passwordless)

Challenge

As a Fortune 50 global, multinational bank, Standard Chartered Bank prioritizes cybersecurity to protect the company’s sensitive PII data and corporate transactions. Having already had multifactor authentication (MFA) implemented for some of its crown jewel applications, the company wished to create a new security control at endpoint desktops and laptops for all bank employees, particularly high-value users such as traders.

SC recognized the fact that bank employees might hold sensitive data on their endpoints, and saw higher levels of remote work precipitated by the COVID pandemic as increasing security risk.

Additional Factors

It was important for Standard Chartered Bank to balance the enhanced security with efficiency - not only for end users in their authentication access, but for the IT security compliance.

Requirements

In addition to the need to meet operational scalability and resilience criteria, SC had several requirements for the desktop MFA solution desired:

- Work with Windows desktops from manufacturers such as Lenovo and Dell, as well as Macs which were planned after a phase one. In general, SC saw the decision as one that needed to create a security control for endpoints in general, whether it were Windows machines or in the future, virtual endpoints.
- Reduce the number of authentication challenges, or "hops", to improve user experience; move from TOTP (timebased OTP codes to mobile push notification for example).
- Integrate and work seamlessly with ForgeRock and the company's user directory which was the Oracle Unified Directory.
- Offer modern authentication factors, such as support for FIDO keys, biometrics and smartphones.
- Support for a non-phone option of authentication – some segment of the bank's users would not be able to use a personal smartphone for authentication.
- Support both passwordless and MFA from one solution – While the end goal is to eventually achieve passwordless, the immediate project scope was for desktop MFA, built on the password paradigm.

Solution

After an exhaustive evaluation of vendors and options, SC chose Secret Double Octopus as its preferred solution for desktop MFA. SC has deployed the Octopus Pro edition of the Octopus Authentication Platform to over 80% of its employees and is targeting deployment to a full 100% of its global workforce in 2022.

In addition, Double Octopus is powering SC's passwordless journey, as the company begins to plan for a full rollout of the Full Passwordless™ edition of Double Octopus (Octopus Enterprise).

"Secret Double Octopus provided the best option for us to deploy a global desktop MFA security control and make progress toward a truly passwordless future."

Kevin Tucker, Executive Director
Head of Privileged Access and Authentication, SC

Why SDO?

Several key criteria and differentiators led to SC's selection of the Octopus solution, including:

- The ability to support 'MFA passthrough' meaning that once a user had authenticated into the desktop, the authentication could act as a "master token" to enable more seamless authentications in other systems, such as a VPN. SC looked for improved user experience relative to its existing authentication workflows, such as for the VPN where time-based OTP codes were used.
- SDO's ability to deploy both MFA and passwordless, which enabled the bank to start with desktop MFA and progress to end-to-end passwordless authentication over time.
- Vendor resilience and responsiveness – SC had many customized requirements that Double Octopus was able to address with its platform.

Conclusion

A trusted partnership for the future!

Standard Chartered Bank plans to continue evolving its identity program with Secret Double Octopus as a centerpiece of its authentication strategy. The company is actively trialing Octopus Enterprise for Full Passwordless™ support across a wider range of use cases.

SECRET DOUBLE OCTOPUS