OneSpan

CASE STUDIES

MOVING MULTI-FACTOR AUTHENTICATION TO THE CLOUD

Stories from financial institutions, fintech, and healthcare organizations who successfully migrated their multi-factor authentication solution to the cloud using OneSpan Cloud Authentication.

EXECUTIVE SUMMARY

Financial Institution:

- Japanese regional bank
- Expanded the functionality of their mobile app
- Improved the user experience
- Enhanced security
- All in a span of only three months

Fintech Organization:

- Retired hardware authenticators
- Provided new mobile app
- Implemented fingerprint biometrics and push notifications
- Improved the user experience

Healthcare Organization:

- Ensured regulatory compliance
- Protected private health information
- Reduced operational costs

Japanese Regional Bank Expands Mobile Banking App Functionality and Boosts User Experience

In November 2019, this Japanese regional bank with 137 branches and $59.33 billion in assets, released their mobile banking application. At first, the functionality of the application was limited and only allowed users to check their balance. Furthermore, the legacy authentication process used in the online channel did not provide a satisfactory user experience. Users would receive a one-time password (OTP) through email and input the password in the web portal. This experience did not translate well to mobile. The bank selected OneSpan to implement Strong Customer Authentication and transaction data signing to securely enable money transfers through the application.

The timeline for this project was exceptionally tight. The bank needed to release the updated version of the app three months after the beginning of the project. Typically, integrating a new authentication solution into an existing app and deploying the on-prem authentication server to support it could take upwards of a year to complete. To expedite the integration and deployment, OneSpan recommended the authentication server be hosted in the cloud.

Now that it is integrated, users no longer receive their OTP through email. They can authenticate by receiving their OTP in-app or leverage fingerprint biometrics. This has created a reliable, secure, and convenient customer experience while expanding the functionality of the mobile banking app.

Norwegian FinTech Delivers Secure Cloud Authentication for All Norwegian Banks

This fintech organization offers Norwegian banks a secure and cost-effective internet security solution for identification and electronic signatures. To authenticate, users were required to use Digipass GO 3 hardware authenticators. Though these authenticators provided the necessary security, user feedback revealed a desire for a software authentication solution that allowed them to leverage their mobile devices. The organization decided to launch a new mobile app to authenticate users with a heavy focus on improving the user experience and to implementing biometrics.

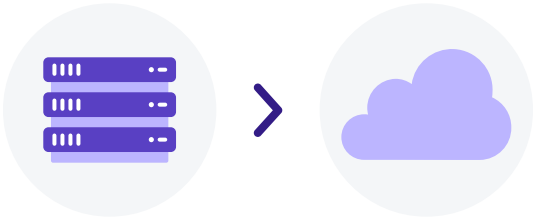
The organization is partially owned by each and every bank in Norway, and they all make use of this service. For that reason, the organization would not even consider an on-premises authentication solution, because this would require each Norwegian bank to provision and deploy a new authentication server on-premises. By leveraging OneSpan Cloud Authentication, the client banks could easily adopt the authentication app without this obstacle.

With the app deployed and banks beginning to adopt its use, users gained access to multi-factor authentication with fingerprint biometrics and push notifications. The new experience proved to be significantly more convenient for the user, and those who downloaded the authentication app could safely retire their hardware authenticators.

Healthcare Organization Introduces Cloud Authentication to Reduce Costs

This healthcare software development company recently modernized their security strategy by adopting cloud authentication. The company sells an Electronic Prescription of Controlled Substances (EPCS) solution that helps doctors and healthcare professionals connect their patients with the regulated medications they need. Due to both the privacy concerns of medical information and the hazardous potential of misusing the medication, authentication is an extremely important component of the solution.

The company migrated from an on-premises implementation to a cloud authentication solution to avoid the costs associated with purchasing, supporting, and maintaining the servers to enable authentication. Second, the company wanted to integrate an authentication process into their existing product using a solution that makes it easy to deploy, evaluate, and verify compliance with all regulations.



OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
OneSpan.com

Last Update October 2020.