Wedding Park Deploys Passwordless Authentication for Internal Cloud Service Logins

Background and challenges leading to deployment

Wedding Park was faced with the challenges of strengthening the security of multiple cloud services that were being used for internal operations and the complexity of password management. As a way to address these issues, the company introduced an ID management service and consolidated them into a cloud service entrance with a single sign-on function.

The impetus for deploying FIDO authentication came from the fact that Salesforce, which is used for authentication for customer management, order and supply systems, and time and attendance management, announced that multi-factor authentication (MFA) was mandatory. However, if MFA is applied only to Salesforce and other cloud services continue to operate with password authentication, not only will the usability of users deteriorate, but the work of the IT management department will also become more complicated. In addition, due to the vulnerability of password-only authentication, the company decided to apply MFA to all cloud services, including Salesforce, in accordance with its policy to promote zero-trust security in February 2020.

Selection and verification of an authenticator

As an authentication method for MFA, the company considered one-time password authentication (OTP) and biometric authentication using smartphone applications, but ultimately decided to deploy passwordless authentication using FIDO for its unique ability to improve both security and user convenience.

In order to realize passwordless authentication using FIDO, a terminal equipped with a FIDO-compatible biometric authentication device is required. The majority of devices currently on the market support FIDO authentication, and with the exception of a few employees, the adoption of FIDO has been supported by the fact that all in-house devices are already equipped with Windows Hello and Touch ID. For some employees who use the devices not equipped with biometric features, a separate external authenticator has been installed.

Corporate overview:

Wedding Park

Wedding Park Co., Ltd. was founded in 2004 with the management philosophy of "Making marriage happier." Celebrating its 20th anniversary in 2024, it started as a wedding review information site and has since expanded its operations.

Utilizing a wealth of information, it operates several wedding-specialized media, including the wedding preparation review site Wedding Park. In addition, it runs various businesses in the realm of weddings combined with digital technology, such as internet advertising agency services, digital transformation (DX) support, and educational ventures.

A step-by-step changeover for each department

After examining the authenticators, the policy to deploy passwordless authentication company-wide in January 2022 was officially launched. The transition took place from February to March of the same year, and the smooth implementation in a short period of one month was made possible by the department-by-department implementation and the generous support provided by the IT management department. For this implementation, the company requested the support of CloudGate UNO, an identity management platform by International System Research Corporation (ISR) that the company has been using since 2012, because it supports passwordless authentication using FIDO2 and biometric authentication using a smartphone APP.

The introduction of the system within the company began with the development department and gradually progressed to departments with a larger number of employees. First, at regular meetings for each department, the company communicated the purpose of why the system was being introduced and the benefits of "the deployment of the system will make daily authentication more convenient," and gained the understanding across the company. The introduction of the system on a departmental basis had the advantage of not only limiting the number of people the IT management department had to deal with at one time, but also allowing the accumulation of QA as test cases and the smooth maintenance of manuals, since the system was introduced starting with the development department, which had high IT skills.

As a result of close follow-up by the IT management department, which not only prepared materials, but also checked the progress status on the administrator website as needed, and individually approached employees who had not yet registered their certifiers, the company was able to implement the system company-wide within the targeted time frame.

Effects of introduction

The number of login errors due to mistyping of passwords, which used to occur about 200 times a month, has been reduced to zero since the deployment of FIDO authentication. Many employees commented that the system has become very convenient, eliminating authentication failures due to forgotten passwords or typing errors. In addition, the number of periodic password reset requests has decreased, resulting in a reduction in man-hours for the administrator.

The passwordless authentication is smooth, and the authentication status retention period was shortened to further enhance security, but the system has continued to operate without problems since then.

Wedding Park's future vision is to link all cloud services used within the company to "CloudGate UNO" and centrally manage them, including authentication, with "CloudGate UNO.

Akira Nishi, General Manager of the Corporate IT Office, who spoke with us about this case study, made the following comments.

"For those who are considering the deploying of a new authentication method, there is inevitably a concern that a change in authentication method will cause a large-scale login failure. In our case, in the early stages of the project, we held explanatory meetings for each department and repeatedly brushed up on explanatory materials and procedures, which was effective in minimizing confusion and anxiety within the company.

"After the switchover, we continued to check on the progress of the implementation and followed up with each department individually, but once the use of passkey (device-bound passkey) became standardized within the company, we felt that the scope of use, including various security measures, was expanding dramatically."