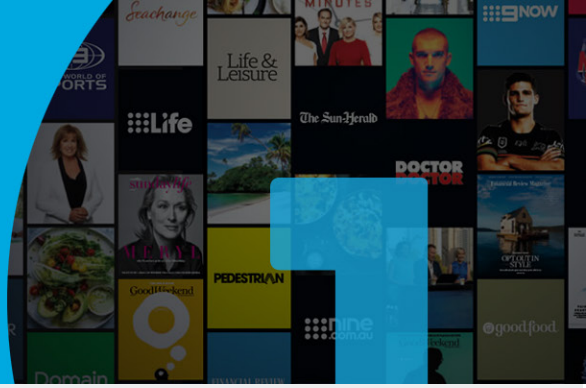
CUSTOMER STORY | Nine

Quickly Adopting and Enabling SaaS Applications, Even During a Major Merger



Nine Entertainment Company is Australia's largest locally owned media company – the home of Australia's most trusted and loved brands spanning news, sports, lifestyle, and entertainment. Nine's assets include television, newspaper, radio stations, digital properties, and a subscription video platform. The company completed a historic $4.3 billion merger with Fairfax Media in December 2018 and generated $1.8 billion in 2019 revenues.

Empowers users to securely and easily access critical applications

Secures and streamlines web application access

Frees small technology team from burdensome maintenance

CHALLENGES

Before the merger, Fairfax had to address challenges like providing secure application access and improving user productivity for employees. Fairfax had initially developed a homegrown single sign-on (SSO) solution, working back and forth with app vendors and implementing SAML themselves. They also built complementary multi-factor authentication (MFA) to support access to various Amazon Web Services (AWS) accounts and other applications.

However, the MFA enrollment process was painful for users and it eventually became a tremendous burden for the technology team to maintain these custom-built solutions. Additionally, as Fairfax deployed more SaaS applications, the team was forced to integrate each app manually with Active Directory (AD). As a result, app rollout was time-consuming, resource-intensive, and often left business users waiting for access.

Meanwhile, Nine had used Azure AD to enable its Microsoft Office 365 and G Suite users. With the merger, Nine inherited the solution Fairfax had chosen to help tame the complexity of ensuring secure and streamlined access to applications that employees rely upon every day.

SOLUTIONS

To meet its growing demands, Fairfax sought a solution that supports integration into a large number of SaaS apps, along with the capability to unify multiple directories in support of its dispersed business units and diverse AD environment. After careful consideration, it chose OneLogin.

Through the OneLogin Trusted Experience Platform™, the Technology team at Fairfax quickly implemented a unified directory, real-time AD sync, network-aware MFA, and out-of-the-box app integration. According to David Tregoning, Systems Architect at Nine, "The rollout went really well and was insanely quick, taking just a couple of days. OneLogin provides some of the best support I've ever experienced with a vendor."

INDUSTRY

Media & Entertainment

USERS

6,550 users

INTEGRATIONS

Adobe Creative Cloud, AWS, Concur, Microsoft Office 365NetScope, Salesforce, ServiceNow, Slack, Smart Recruiters, ZenDesk

"OneLogin has been our Identity and Access Management tool of choice for years and continues to be. It's how we make sure our people and brands are protected."

David Tregoning
Systems Architect

When the merger went into effect, OneLogin became the standard Identity and Access Management platform for Nine. To date, Nine is using 200+ OneLogin connectors to support access to about 50 apps and numerous WordPress sites associated with the company's custom-built publishing system hosted on AWS.

RESULTS

As of early 2020, about 6,550 active Nine users are on OneLogin. While everyone in the company is associated with both an Azure and OneLogin identity, the identity rolls through OneLogin whenever possible.

With OneLogin's Desktop SSO feature in place, users are no longer prompted for MFA – the authentication happens seamlessly. In fact, end-users are unaware they are even using OneLogin's Desktop SSO solution, which uses integrated windows authentication to automatically log users into the OneLogin Portal. End-users directly and securely access the applications they need from a single, easy-to-use portal. "Users shouldn't need to worry about identity and access management, and they don't need to with OneLogin. We on the Technology team know that OneLogin is in place and doing its job, and that's all that matters," says Tregoning.

SmartFactor Authentication™, OneLogin's adaptive MFA offering, removes a point of friction when staff log in to applications by suppressing MFA when the risk is low. This context-aware product knows when users are logging in from their default machine, even if they are logging in from a different location – such as their home office – and analyzes typical user behavior to suppress or enforce MFA depending on the level of risk for each login attempt. If a user isn't yet enrolled with MFA, they're walked through a self-service, wizard-based enrollment process.

This is especially valuable now that more employees are working from home and are accessing their applications on multiple devices and from different locations. "With our small team, just two of us can easily manage OneLogin for our thousands of users," explains Tregoning. Moreover, it's easy for the technology team to quickly add new applications and users as the need arises.

"Our belief is that any web-based application should authenticate via OneLogin. OneLogin has been our Identity and Access Management tool of choice for years and will continue to be so. It's how we make sure our people, data, and brands are protected," concludes Tregoning.

- Relieves support burden while strengthening security
- Empowers users with efficient single sign-on and self-reset passwords
- Faster app rollout better supports the business