IT service provider in EMEA turns to Datawiza to add MFA to Oracle JD Edwards

Datawiza enables business to easily comply with requirement for multi-factor authentication for critical business applications running in Microsoft Azure Cloud – in just a few days

BENEFITS

- MFA compliance was achieved in a matter of days

- Easy to test and implement with a free (full) version

- Reduced costs by leveraging existing investment in Microsoft 365

CHALLENGES

- Enable Microsoft 365 MFA for Oracle JD Edwards (JDE)

- Meet MFA compliance requirements ASAP

- Limited resources and budget

> " After testing Datawiza with the free version, the company's IT manager said he could not have imagined there was such an easy and cost-effective solution to the challenge of adding MFA to critical business applications. After implementing the full Datawiza solution to enable MFA for all users, the company has now experienced our Datawiza support – and our IT contact was nothing short of delighted. The team is looking forward to securing other applications on other cloud platforms with Datawiza. "
>
> **Canming Jiang,** CEO, Datawiza

Time challenge: How to quickly add multi-factor authentication to cloud-deployed Oracle JD Edwards

As cyber threats continue to strike terror in hearts of the C-Suite, businesses are under extraordinary pressure to up their cyber defenses – and fear isn't the only motivator. Businesses also need to comply with evolving regulations and cyber insurance requirements around the world.

This is the environment faced by a major IT solutions provider in EMEA. The company has long relied on Oracle JDE for enterprise resource planning – a mission-critical capability for a company that counts on partners and an efficient supply chain to meet its obligations to customers and deliver excellent customer service. Because the company maintained only a small internal IT shop, it opted to deploy JD Edwards on Microsoft Azure AD to eliminate the need to maintain an on-premises infrastructure and purchase, configure and maintain new hardware as its needs grew.

This was an effective solution until growing cyber threats and evolving governmental regulations demanded that the company add multi-factor authentication (MFA) to applications that expose sensitive data to the internet.

As a "legacy" application, JD Edwards has no built-in support for modern security protocols (SAML and OIDC/OAuth), which enable MFA for modern SaaS applications.

This meant that users anywhere in the world – using any type of unsecured device – could access the company's JD Edwards application with a simple username and password, which can be easily phished or hacked. In fact, according to Microsoft, 99.9% of the compromised accounts they track every month lack MFA, which stops most automated account attacks.

- To improve its security posture and satisfy the government-mandated compliance requirement for MFA, the company at first thought it had only a handful of very expensive and time-consuming options: Replace JD Edwards – requiring months to years of retooling and retraining
- Use legacy but very expensive access management solutions, like Oracle Access Manager (OAM) or F5 Access Policy Manager (APM)
- Hire a system integrator

These time and cost challenges were not limited to just the initial projects. Each option carried with it an expensive and time-consuming maintenance requirement. And when the company wanted to extend MFA to other applications, the entire process would start over again.

From "Try for Free" to a full implementation

Frustrated with these choices, the company's IT manager tried a simple Google search – "Add MFA to JD Edwards" – and immediately found a link to Datawiza's solution page for adding MFA to JD Edwards, as well as technical videos for how to implement it.

Intrigued, the IT manager reviewed in detail the information on the Datawiza website. Datawiza provides a no-code platform for easily integrating any applications with Azure AD and other cloud platforms. Datawiza acts as a bridge between the application and the identity platform, enabling businesses to centrally manage support for MFA, as well as single sign-on and conditional access, across all their applications, located anywhere – in multiple public and private clouds and on-premises. Datawiza was also built by an experienced team with deep security expertise.

Impressed by the simplicity of the solution and the pedigree of the company, the IT manager opted to click on the Datawiza "Try for Free" button, and in just a few minutes, he created and configured an account and launched a proof of concept, which worked exactly as he had hoped. He then began using Datawiza to implement MFA for the JD Edwards production environment for a limited number of users.

This limited use of Datawiza proved so successful, that within a few weeks, the company contacted Datawiza to see if it made financial sense to adopt the full version of Datawiza both as a short-term solution for compliance with the MFA regulation and as a long-term solution for protecting other critical applications. The company learned that Datawiza works with any application, not only legacy apps, but also modern cloud-based apps. The solution would also require zero maintenance on the part of the company's IT team, no matter how many applications were protected or which cloud platforms they were deployed on. This capability, combined with excellent support from the Datawiza team, led the IT manager to implement the full version of Datawiza.