

Enabling a secure and scalable multi-factor authentication platform for a US-based, not-for-profit organization with Azure Active Directory



Case study



Client

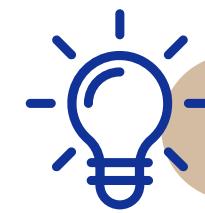
The client is a not-for-profit organization in the field of alternative dispute resolution, providing services to individuals and organizations that wish to resolve conflicts out of court and one of several arbitration organizations that administers arbitration proceedings. Additional services include designing and developing alternative dispute resolution (ADR) systems for corporations, unions, government agencies, law firms, and courts.

The existing client infrastructure consisted of Oracle's security solution leveraging Oracle Identity Manager for the identity life cycle management (LCM) process, along with custom scripts for users to create, modify, delete, enable, disable, password reset, and more.



Challenges

- Need for a cloud platform solution to strengthen security, agility, scalability, and a cost-optimized MFA solution
- Multiple custom scripts/solutions on top of the Oracle Identity Manager for handling identity life cycle events
- No centralized authentication - application users authenticated via Oracle Identity Directory (OID) or Oracle databases
- Lack of single sign-on solutions
- Lack of multifactor authentication



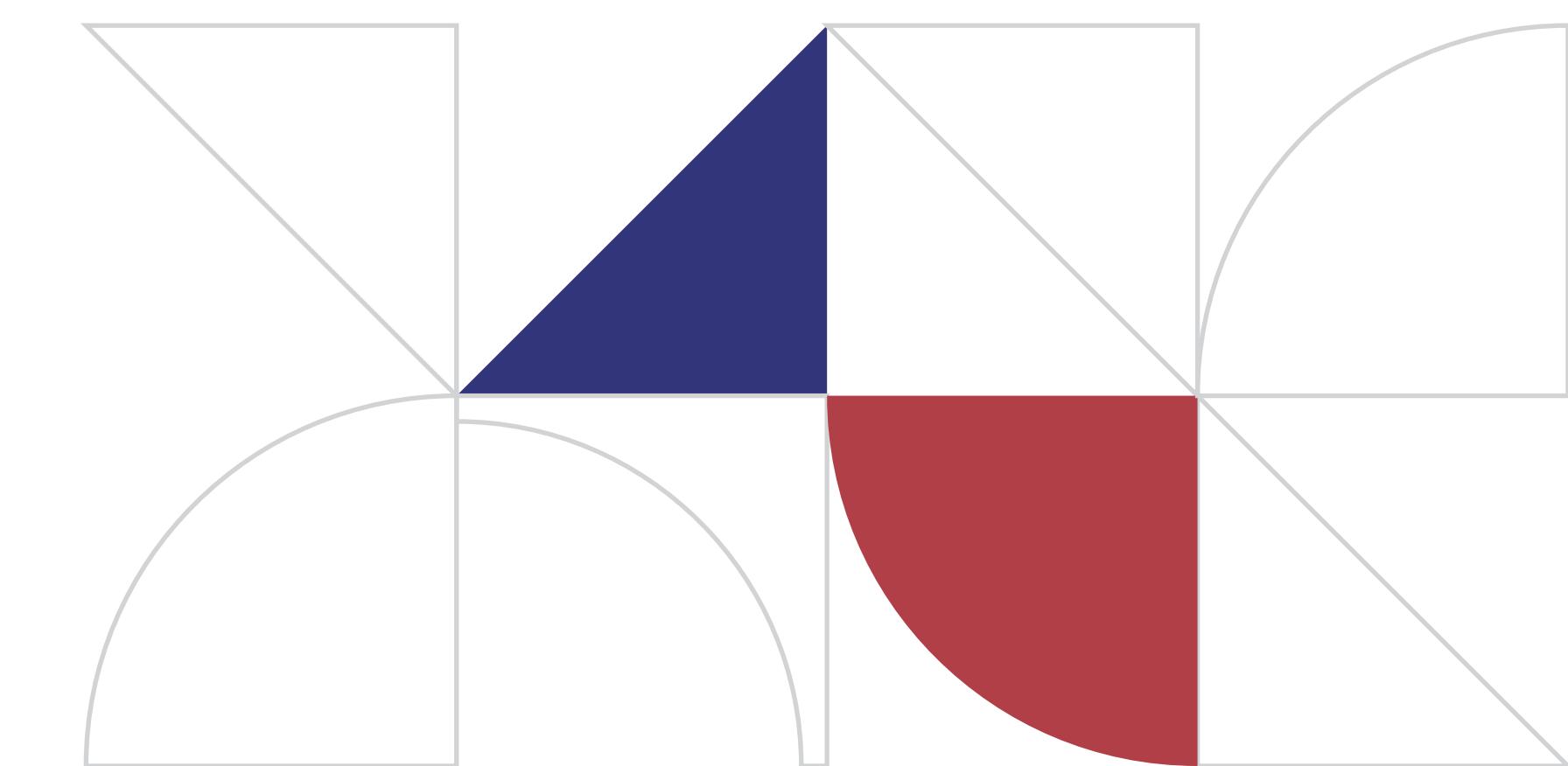
Solution

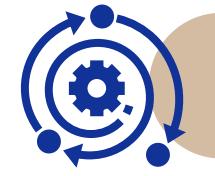
We helped the client save costs through cloud migration security services and meet all major security compliances.

First, we conducted an eight-week assessment to understand the existing OID solution. Next, we created a plan to facilitate the migration process to Azure Active Directory (AAD).

We conducted the following activities:

- Served as the intelligent migration advisor to design and implement the secure, agile, and scalable Azure AD solution
- Migrated users from Oracle Internet Directory to Azure Active Directory
- Enabled multifactor authentication
- Migrated identity LCM processes from OID/Oracle databases to on-prem Active Directory
- Synchronized and created hybrid IDs with AD connect cloud sync for the users in Azure Active Directory





Business impact

- Multifactor authentication enablement using Azure Active Directory
- Seamless user login single sign-on experience
- User sync and hybrid IDs on Azure AD for both internal and external user identities
- Migration from Oracle Internet Directory to on-prem Active Directory/Azure Active Directory
- Scope for future scalability to migrate on-prem applications to Azure Cloud





We conceptualize, build, and manage digital products through experience design, data engineering, and advanced analytics for over 130 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile, and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,000+ associates work across 33 locations, including San Jose, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

For more information please contact: velocity@zensar.com | www.zensar.com

