# AUTOMATED IDENTITY SYSTEM INCREASES EFFICIENY AND SECURITY

how upgrading from a home-grown identity and access management system saved time and resources and increased security for this Midwest-based manufacturer

CASE STUDY: IDENTITY & ACCESS MANAGEMENT

zirous®

zirous®

## OVERVIEW

Managing internal and external user access to applications improves efficiency and mitigates the risks of a security breach.

## THE CHALLENGE

This Midwest-based window and door manufacturer first implemented an Identity and Access Management solution as a way to consolidate their customers' access across several external applications. Before that point, customers maintained different identities within each system and the manufacturer was unable to correlate their access or activities.

After the success of this project, the business units recognized the benefits of applying the same technology, but internally. The manufacturer had various inefficiencies with their legacy Identity and Access Management system, including:

- No user self-service functionality for various access requests;
- Password storage vulnerabilities;
- Requiring many user logins across multiple business applications; and
- High level of effort in order to maintain the customizations in the old system.

Because of these pain points, the manufacturer recognized the need for an enterprise solution that would make both provisioning and access management easier to use and mitigate the security issues from the home-grown legacy system. The new solution would position them to perform role-based access control, which would lead to faster and more accurate access provisioning and deprovisioning. Additionally, the solution would support single sign-on across applications - to both internal and cloud applications - to standardize and simplify the end user experience.

## THE SOLUTION

Zirous led the design and execution of a multi-year roadmap to implement a solution integrated with several key internal systems. The solution was broken into phases based on impact, business priority, and complexity of the systems being replaced.

The first phase focused on identifying and cleansing multiple accounts to create single identities. This process identified which persons owned accounts in various systems. Previously, user logins might not have been consistent across systems, which made it hard to understand what access a person had. The consolidation of identities also provided a foundation to support single sign-on.

Single sign-on was implemented across systems, including a cloud-based HR tool. The solution included the ability to prompt for step-up authentication, depending on the sensitivity level of the system. In other words, walking by an unlocked PC wouldn't give a person with malicious intent the ability to automatically log into any and all sensitive systems.

OIM was configured to provision and deprovision internal AD and EBS accounts in a timely manner. This facilitated the replacement of an aging legacy automation tool. It also used Role Based Access Control (RBAC) to automatically provision

## QUICK FACTS

Company
- Midwest-based window and door manufacturer
- Products sold throughout the U.S.
- Over 6,000 employees

Technologies Involved
- Oracle Identity Manager
- Oracle Access Management
- Oracle Internet Directory
- Oracle HTTP Server
- Oracle WebLogic Server

## HIGHLIGHTS

- Midwest-based manufacturer had inefficient, home-grown identity and access management system.

- The company recognized the need for an upgraded solution to mitigate risk.

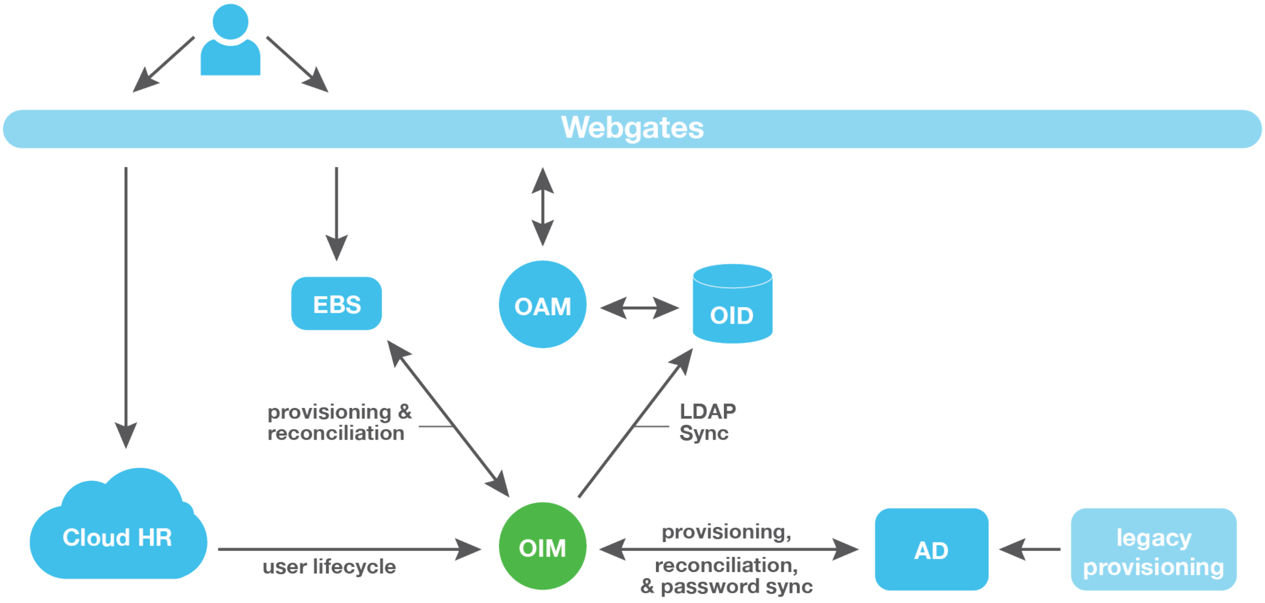
- Single sign-on was implemented, improving efficiency and security.

- Automated provisioning reduces inefficiencies during the onboarding process.

- Automated deprovisioning reduces risk by removing access immediately.

birthright access as part of the process of onboarding new employees. Additionally, the solution ensured that accounts were disabled in a timely manner when a person separated from the company.

In order to make the new system more dynamic and easier to maintain for the manufacturer, Zirous' intellectual property was leveraged to create and modify accounts. Changing decisions on where in Active Directory to provision a user, for example, only required an update to a spreadsheet rather than time-consuming code changes.



## THE IMPACT

The enterprise solution for this Midwest-based window and door manufacturer has greatly improved the employee onboarding process by reducing the number of manual processes and bringing efficiencies in multiple areas.

Today, new employees can get immediate access to the company's HR system using their identity account and the same password they use to log into their PC. The company now has challenge questions set up as a required part of on-boarding, and no longer needs to burden the help desk staff with password reset requests when employee passwords are forgotten. The help desk can also use OIM to handle requests for access instead of having to reach out into different systems to grant the requested access.

Concerns about keeping passwords in sync across systems are no more and the significant security risks of the home-grown SSO tool have been eliminated. The complex custom code of the home-grown provisioning and SSO solution are on track to be eliminated and replaced with standardized processes, freeing up IT resources that had previously been performing endless maintenance.