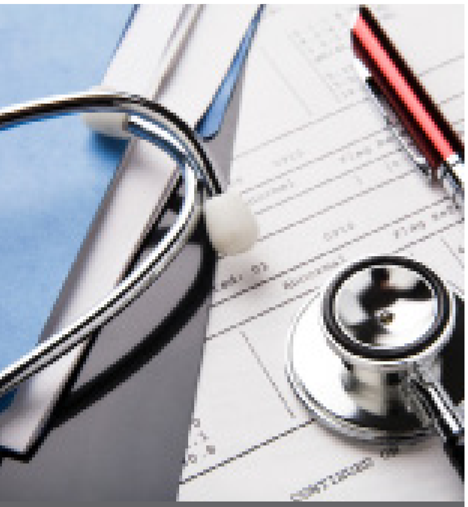
Midwest Healthcare Insurance Company



Overview

Oracle Identity Management allows enterprises to manage end-to-end lifecycle of user identities across all enterprise resources both within and beyond the firewall. You can now deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and much more. Oracle Identity Management is a member of the Oracle Fusion Middleware family of products, which brings greater agility, better decision-making, and reduced cost and risk to diverse IT environments.

Healthcare organizations today must manage two diametrically opposed sets of requirements: the practitioners' need for easy access to information versus the business' need to apply increased privacy and security controls against that data. On top of this, the rise of technology and its adoption into the healthcare field has caused healthcare organizations to accumulate a variety of non-interoperable systems that not only need to work together within the organization, but are also accessed from outside. With regulations such as HIPAA, Sarbanes-Oxley and the Graham-Leach-Bliley Act, information security and recertification has become a key initiative in healthcare companies.

With nearly 200 applications having multiple environments and 2500 users, this Midwest Healthcare Insurance Company could no longer effectively manage their recertification and provisioning process manually. They estimated annual expenditures in excess of $1,500,000 to meet their compliance requirements. A solution that reduced costs, simplified process and increased the dissemination of tasks and associated privileges for a specific business process among multiple users was essential to continued success. Leveraging the features of Oracle's Identity and Access Management Suite, Zirous designed and implemented a solution that dramatically reduced costs, simplified recertification, automated user provisioning and provided segregation of duties which eliminated unauthorized access permissions.

Challenges

Automating the complex process of any large company can be challenging. This company's primary challenges include:

- **No use of roles** to provide access to users
- **200 applications** on a variety of platforms
- **Externally hosted** mainframe environment
- Complex **segregation of duties** and **request approval** requirements
- Time consuming recertification process

Technology Stack:

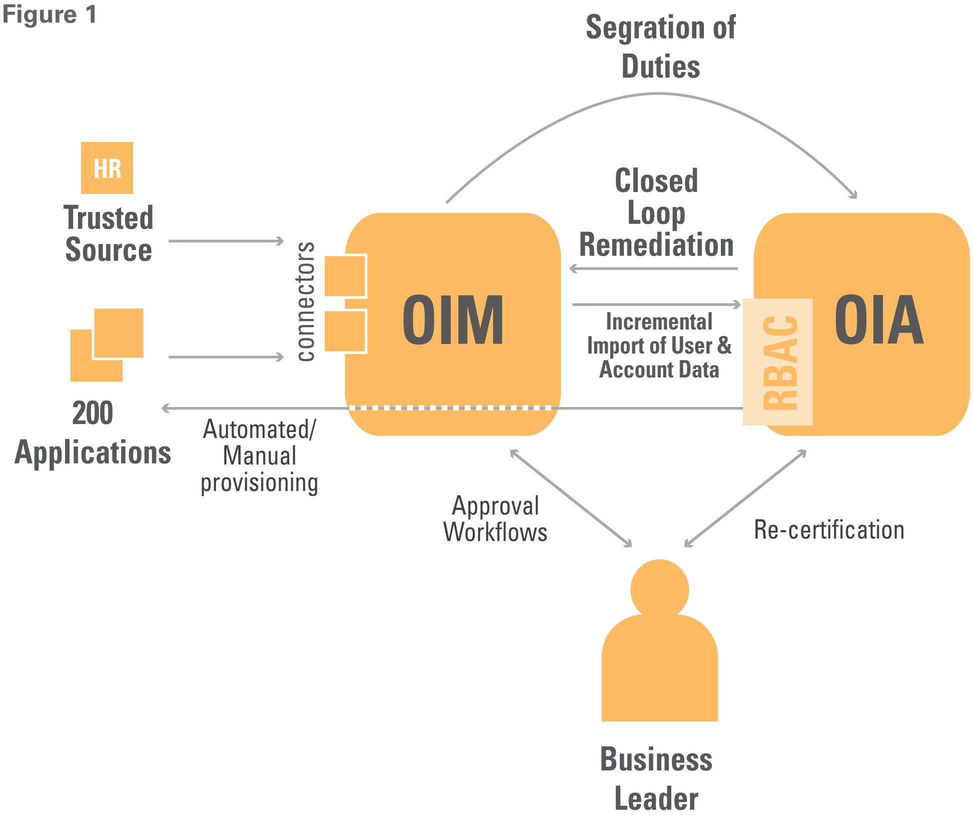
Oracle Identity Manager 11g
Oracle Identity Analytics 11g
Oracle Business Intelligence Publisher
Oracle WebLogic Server 11g
Oracle Database 11g

Solution Details

Zirous architected a solution leveraging key features of Oracle Identity Manager (OIM) and Oracle Identity Analytics (OIA) (Figure 1). Highlights of the solution include:

- Segregation of Duties: Eliminate unauthorized access permissions, including Protected Health Information (PHI) violations and dangerous combinations
- Role Based Access Control (RBAC): Increase security through pairing business functions with system access
- Recertification: Increase user experience by decreasing leader time spent in both request and recertification efforts
- Provisioning: Decrease errors through automated user provisioning
- Request Approval: Decrease security administration time spent determining and gathering required approvals for access requests through approval workflow automation.

Figure 1



The company's applications utilized Microsoft Exchange, Microsoft Active Directory, ACF2, internal and external identity database structures or a combination of sources to identify authorization and access control. Due to the lack of use of roles to define access and authorization, the solution required significant analysis to determine the most effective way to provide RBAC.

The biggest cost benefit was a result of the implementation of automated quarterly, bi-annual, and annual recertification processes. These processes implemented in OIA are estimated to save $1.3M annually. It is based on certifying access using the following certification types:

User - Leaders approve employee roles and any access that is outside of a role
Data - Owners of specific entitlements approve the users with access to the entitlement
Role - Role owners certify the access associated to each role

Closed-loop remediation occurs at completion of the recertification process. Any access changes will trigger a de-provisioning process in OIM improving overall security and decreasing compliance costs.