

Healthcare Major Adopts Role-Based Access Control



Case Study

Customer Profile:

A major healthcare provider based in the United States. The company is mission-driven to improve affordable access to health care. It is a not-for-profit, policyholder-owned company.

No of users: 10,000.

Business Drivers: Meeting compliance and regulatory requirements for access certifications.

- **Wide range of applications:** The organization uses a wide range of applications and systems in order to support the business needs of its employees. Given the complexity of its IT environment, manually certifying user access on each application and meeting compliance deadlines posed a huge challenge.
- **Lack of a central repository:** The Company lacked a much-needed centralized repository, which would provide a single view of all the users and their access across all the critical applications.
- **Regulatory compliance:** The Company has to meet various regulatory requirements such as HIPAA, SAS 70 and MAR (Model Audit Rule) to demonstrate compliance. This involves certifying user access across a wide range of applications on a quarter to annual basis.

Addressing these needs required significant investment of time, money and people. The healthcare major saw an immediate need for an identity management solution to optimize its access certification process.

The Solution:

The company appointed Simeio Solutions to recommend and integrate an identity management solution, which would effectively address all the requirements.

Simeio Solutions presented a proof-of-concept to demonstrate the capability of a role-based access control solution to do the following:

- Build a centralized repository of all users
- Select the critical applications
- Provide a single view to analyze users and access to critical applications
- Automate access certification for data owners

The proof-of-concept convinced the client that the role-based access control solution would be a fitting answer to its compliance needs.

After initial meetings, which involved company stakeholders and the Simeio implementation team, an action plan was drawn up. Simeio began with gathering data to populate the identity warehouse or the central repository of users. Simeio used detailed questionnaires and meetings with application owners and stakeholders to gather the data.

Simultaneously, the Simeio team analyzed the certification requirements and inferred that the out-of-box certifications would not fit the requirements of the organization. Therefore, a hybrid certification process was developed. The two-step certification model involved a review of user's access by a cost manager and then a sign-off by business owners of the application.

Lastly, Simeio designed various custom reports to help the company monitor certifications and user access.

The organization is now able to monitor user access across its wide array of applications in an automated and effective manner.

Implementation Highlights:

Simeio's expertise played a critical role in the success of this implementation. Some of the highlights included:

- Quick understanding of the security model of diverse applications and ability to seamlessly liaison with technical and business teams spread across multiple business units.
- Developing a custom access certification process designed to fit seamlessly into the existing business processes.
- Conducting an in-depth and hands-on technical training in order to make the organization self-reliant.
- Meeting aggressive project timelines thereby enabling the organization to meet its compliance deadlines.
- Demonstrating a significant Return on Investment (ROI) in a short span of time.

Future Prospects:

Having experienced the value of a role-based access control solution, the organization is now gearing up to implement two key modules: *Role Engineering*, which involves defining roles for the enterprise, and *Role Management*, which would entail processes such as role consolidation, role provisioning and role de-provisioning.

The company is also actively seeking a provisioning solution to remediate user access and run audit scans for Segregation of Duty (SoD) violations within and across multiple applications in the enterprise. It is also planning an Enterprise Role Definition project.

About Simeio Solutions:

Simeio Solutions LLC is a systems integration and compliance consulting company specializing in enterprise security. The company provides consulting, implementation and management services in the areas of identity access management (IAM), role-based access control (RBAC), and governance, risk management and compliance (GRC). Simeio is headquartered in Hoboken, New Jersey and counts numerous Fortune 1000 companies among its clientele. For more information, visit www.simeiosolutions.com or email at info@simeiosolutions.com

East Coast Operations:
Hoboken Business Centre
50 Harrison Street, Suite 314
Hoboken, NJ 07030

West Coast Operations:
3900 Kilroy Airport Way
Suite 270
Long Beach, CA 90806