Health Insurance Provider

Core Compliance

Large health insurance provider selected Core Security's Core Compliance solution to:

- Streamline the attestation process
- Eliminate shared accounts
- Improve compliance metrics
- Have the ability to demonstrate HIPAA compliance

Background

This Core Security customer is a health insurance provider that was facing two major challenges in meeting its user access compliance requirements: frequent audit failures and high process costs. The main root cause of these issues was a largely manual attestation process that was not meeting the business' compliance requirements.

The Challenge

Most of the sensitive data for this is organization is stored in three key enterprise systems. These target applications and systems require periodic review to ensure that least privilege access is given to the users to meet their job functions. At each review, the IT Security team first had to separately extract and compile user access data from the target systems. The compiled data was prepared and sent to the intended managers for attestation. Upon receiving the attestation reports, the IT Security team then organized the reports for audit.

This process, due to its multitude of manual steps, inevitably introduced errors and inconsistency, resulting in inaccurate reports and less than desired audit findings. The IT operation at the company is outsourced, which adds to the cost of the process, and any corrective activities at any stage of the attestation process increased costs even further.

To address these challenges, the company chose Core Compliance to automate its compliance process.

The Approach

The Core Security solution implementation starts with building a data infrastructure that serves as the attestation platform. Using Core Compliance, Core Security's compliance management solution, workflows are configured to display data through a Web user interface.

There are five parts to the solution:

1. Receiving and preparing review data for presentation to the managers and the resource owners
2. Creating a responsibility hierarchy so that a manager or resource owner is only presented with review data that belongs to his/her attestation responsibility
3. Capturing and presenting previous review attestation and comments
4. Storing and capturing of attestation review
5. Notification to Security Administrator or resource owner if changes are to be made.

The solution provides the following features and functionality

Scheduling and Escalation:

- Reviews are scheduled and reviewers notified (Managers, Resource Owners)
- If a review is not completed by a reviewer within the requested time frame, reminders are issued and the review is automatically escalated up to 3 levels.

Manager Compliance:

- Can review staff up to two management levels deep in their department
- Can review all systems access of a user
- Displays active accounts of terminated users
- Displays staff with administrator access
- Manager can attest, remove, or modify access

Resource Owner Compliance:

- Owner selects resource to review if they own more than one
- All users with access to that resource are displayed, along with access entitlements
- Resource Owner can attest, remove, or modify access

Compliance Metrics:

- Reviews completed
- Reviews outstanding
- Escalation status

The company completed extensive user testing on the solution and moved to production eight months after purchase. The deployment started with a small pilot group, followed by gradual phasing-in of the solution to all users over a period of six months.

The Result

Preliminary compliance reviews highlighted a large number of shared accounts that should not exist, and therefore further investigation and cleanup was deemed critical by the organization. Not only were accounts available to those that should not have access to such information, but many existing records of resource owners were found to be erroneous or incomplete. Without Core Compliance, the company would not have identified these compliance violations and therefore are on the way to achieving continuous, automated compliance in accordance with internal policy and healthcare industry regulations.

ABOUT CORE SECURITY

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

World Headquarters
COURION CORPORATION
1000 Holcomb Woods Parkway
Suite 401, Roswell, GA 30076

Phone: +1 508-879-8400
Toll-free: 1-866-COURION
www.courion.com

CORE SECURITY