CASE STUDY

SEA™ SOFTWARE ENGINEERING OF AMERICA

Heartland Finds the Key to Security Compliance

SUMMARY

When the previous security software vendor couldn't keep up with the expanding requirements of Heartland Financial USA, Inc., the banking institution looked for a vendor that offered a wide array of automated security products with the features and functionality to match the regulatory demands of multiple auditing teams. As you know, when the auditors are asking for quality assurance you can't provide, there's a real incentive to change things for the better.

Heartland FINANCIAL USA, INC.

SEA helped Heartland solve four of its biggest auditing and reporting challenges by integrating iSecurity products into Heartland's IBM i security scheme:

1. **iSecurity Audit** allowed Heartland to produce a wide variety of audit-ready reports for its IT managers, security teams, and its internal and external auditors. iSecurity Audit increased the quality and quantity of their reporting and helped automate the reporting process.

2. **iSecurity Authority on Demand (AOD)** allowed Heartland to control the overuse of elevated and security officer privileges and to regulate access to Heartland's IBM i systems, providing better security and answering the company's auditing requirements.

3. **iSecurity Firewall** answered Heartland's need to lock down access to its financial information system from internal users using techniques such as FTP, preventing unauthorized local intrusions into IBM i data, along with identifying and report ing in real-time on company users trying to access secured data.

4. **iSecurity Password Reset** provided users with a self-help system for quickly resetting disabled IBM i passwords by using two-factor authentication. Password Reset reduces Help Desk time assisting users who are locked out of the system, freeing up human resources that can be concentrated on strategic IT projects rather than simple password resets.

This combination of products heightened IBM i security for Heartland's sensitive data, and it gave Heartland the tools it needed to document the security policies for the company's management, security team and its auditors. With the new tools, Heartland not only implemented great IBM i security, they could monitor and report on that security to anyone who asked.

Here's how Heartland met these goals.

PROBLEM

The security software Heartland previously used was not being regularly updated and it couldn't adequately match Heartland's need to answer requests from its internal and external auditing teams. Heartland was limited in what types of security reports it could produce; the company needed more flexibility for the systems and its auditors.

Heartland's IT operations staff is responsible for daily, weekly, monthly and on-demand security reporting. Most reporting is delivered via email, while some reports are printed and archived for IT managers who sign-off on reports before they are presented to the auditors from the Federal Deposit Insurance Corporation (FDIC), Sarbanes Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS) and in-house auditing teams. Additional reports are sent to the Heartland IT security team.

Heartland was also searching for security software that went beyond reporting, which was the only functionality Heartland's previous software provided. Heartland didn't just need to report on their security efforts, it needed and wanted to improve on its security efforts.

In addition to expanding its reporting capabilities, Heartland needed to control and monitor users with elevated access privileges to its financial data, a risk that was identified by the auditors from the FDIC. Other security needs included preventing network users from accessing internal IBM i data using common methods, such as FTP.

SOLUTION

A security strategy is an ongoing process. Regularly scheduled security assessments will likely lead to altered security objectives. There is no single-tool solution or end-point that puts a cap on vulnerabilities. Heartland, with input from the auditors most familiar with the company, set a goal of prioritizing its top concerns, identifying risks and determining which security processes could be put in place to manage risk and solve current business problems.

Fortunately, Heartland's core business applications run on the IBM i operating system, a highly securable system that provides a rock-solid framework for deploying security software. Equally fortunate was the discovery of the iSecurity software and the security experts on staff at SEA.

After reviewing several IBM i security products, Heartland chose four iSecurity modules: Audit, Authority on Demand (AOD), Firewall and Password Reset. These products would help Heartland achieve its goals of better identification and neutralization of security risks, improving security, clamping down on excessive authorities to IBM i data and providing wide-ranging and flexible reporting for auditors.

RESULTS

Jane Roussel is the computer operations applications lead at Heartland. Her responsibilities include support for the core applications running on the IBM i system including security and all things related to the IBM i system. She managed the deployment of the iSecurity software on Heartland's IBM POWER8 servers with production and LPAR test environments. The system runs on IBM i 7.3, the latest version of the operating system.

Roussel is pleased with the results of the software. Here's how she rolled out her new capabilities:

iSecurity Audit – To eliminate any confusion or disruption, Roussel began by determining which reports from her old security software were no longer necessary and eliminated them. She then duplicated the requisite reports provided by the previous vendor into iSecurity Audit and added new reports that were requested by the auditors that the previous vendor software couldn't produce. Some printed reports were replaced by Excel documents attached to emails for faster distribution and ease of use by the recipients, including the Heartland IT managers and security team along with the company's internal and external auditors. Most of the reports go to IT managers and are later presented to the auditors. The query and reporting features included with the product were a major enhancement compared to the capabilities available in the previous product, as reports could be quickly generated for new requests.

iSecurity Authority on Demand (AOD) – The Authority on Demand module enabled Heartland to control the overuse of elevated IBM i security access, an issue that was high on the priority list of IT managers after auditors brought it to their attention. AOD identifies which users have access to what data, and determines what level of access they have and what level of access they should have.

Heartland's goal was to assign the lowest level of authority required to successfully run the applications necessary to do their jobs. AOD tracks users in real time and monitors what they are doing and when they are using elevated access. No one uses elevated access without it being monitored. If elevated access is used, email alerts are generated to security personnel. AOD raises the level of accountability, limits the amount of accessibility and satisfies auditors' request for clamping down on this security vulnerability.

iSecurity Firewall – The value of this module, Roussel says, is that it locks down another avenue to information access. The Firewall product provides more control over who can use FTP and other remote access methods, and who has read-or-write privileges. Reports are sent in real time when attempts to access unauthorized files are denied. Firewall identifies internal users who are trying to access off-limits data.

iSecurity Password Reset – "I've heard great feedback from people that have used this feature," Roussel says. The Password Reset module takes reset requests from users who forgot their passwords or locked themselves out. The software uses two-factor authentication to authenticate users and enable them to unlock and reset their passwords without help desk assistance, essentially becoming an automated self-help desk. Users are happy because they get quicker resolution to their password problems and the Help Desk gets relief from calls that prevent them from resolving more important issues.

CONCLUSION

Using the iSecurity software has made a big difference for Heartland, helping it to meet its security and auditing goals.

The iSecurity Authority on Demand and Firewall modules provide more control and visibility over who accesses IBM i data and when unauthorized accesses occur, with the capability to detect security violations in real time. The iSecurity Audit reporting capability is miles ahead of Heartland's previous solution, with over 200 ready-to-run report templates for easy audit and security forensics report generation. iSecurity's Password Reset module provides users with a quick and easy self-help way to reset their passwords, taking IT resources out of the password reset process.

"Right now, we are very happy with what we have. [The iSecurity software] addresses all the requests from the auditors and what we want internally," Roussel says. "And SEA's support is wonderful. They were always very responsive. Implementation and deployment questions were handled quickly. Support is important, especially with security software. They were there to hold my hand when I needed it."

About Heartland Financial

Heartland Financial USA, Inc. is multi-bank holding company offering banking solutions for business and personal clients. Heartland's independent community banks are chartered in the states of Iowa, Illinois, Wisconsin, New Mexico, Arizona, Montana, Colorado, Minnesota, Kansas, Missouri, Texas and California, with a total of 118 banking locations serving 89 communities.

About Software Engineering of America (SEA)

SEA is a leader in datacenter software solutions with products licensed at thousands of installations worldwide. More than 10,000 data centers of all sizes and configurations are utilizing one or more of SEA's products, including nine of the Fortune 10 and 85 percent of the Fortune 500 companies.

SEA

SOFTWARE ENGINEERING OF AMERICA
PHONE 516.328.7000 SALES@SEASOFT.COM WWW.SEASOFT.COM