CASE STUDY

SIRIUS HELPS A HEALTH BENEFITS COMPANY STREAMLINE USER ACCESS AND SECURITY WITH A SINGLE, HIGHLY SECURE PORTAL

THE CLIENT

A diversified health benefits and information company.

THE CHALLENGE

The client has about 2,500 users across four facilities who need access to a variety of different applications including financial, administrative, HR, claims and healthcare systems, not to mention technical and IT staff who require very deep access into databases, platforms and operating systems.

THE SOLUTION & RESULT

A proprietary, branded interface integrates functionality from a broad range of tools and technologies from the IBM® Security stack, including IBM Security Identity Manager (ISIM), IBM Security Access Manager (ISAM), IBM Security Federated Identity Manager (FIM), IBM Security Privileged Identity Manager (PIM), IBM Security Access Manager for Enterprise Single Sign-On (ESSO), and IBM Security Identity Governance and Intelligence (IGI).

The client now has a single interface for identity management instead of four, which dramatically simplifies the process of applying for access privileges and helps the company meet government and industry information security regulations such as HIPAA and HITECH.

It is Sirius policy not to identify clients featured in security case studies.

Few industries have such strict security requirements as healthcare. With strict and evolving industry and government regulations such as HIPAA and HITECH, healthcare providers, health insurance companies, pharmacies and other related businesses must safeguard patients' protected health information (PHI) from both external threats and improper internal access.

Until mid-2016, one Sirius client had four methods by which users could request access to applications, which was both confusing and frustrating to staff, and created a heavy burden on administrators who had to determine who could or should have access. Users didn't know where or how to request access, which interface to use, what they had to request access to, whom to call for help, and how long the process would take. Each request could require approval by up to eight individuals, and the system was receiving an average of 11,000 requests per month. And there wasn't a reliable method for promptly revoking all access privileges to users who left the organization. For a company in the healthcare industry, this was an unacceptable risk, and a huge administrative burden.

When it began working with Sirius to blueprint a single, comprehensive identity management solution to replace its legacy systems, the company's guiding questions were: Who actually works at the company, and how do we know for sure? What access do they have? Is the access appropriate to their job function? And do we know in real time when users end their relationship with us?

With the help of Sirius' Security Consulting practice, the client has consolidated four identity management systems into one user-friendly, branded interface. That interface is the culmination of analyzing and migrating hundreds of services into a one-stop shop for security access requests, fulfillment, and often automated provisioning. This implementation is distinguished by the quantity of applications migrated from legacy systems and the sophistication of the holistic solution for identity management, governance, and federation.

When it is fully implemented, the solution will integrate functionality from a broad range of tools and technologies from the IBM Security stack, including IBM Security Identity Manager (ISIM), IBM Security Access Manager (ISAM), IBM Security Federated Identity Manager (FIM), IBM Security Privileged Identity Manager (PIM), IBM Security Access Manager for Enterprise Single Sign-On (ESSO), and IBM Security Identity Governance and Intelligence (IGI).

The interface gives the client's administrators full visibility into all elements of identity management, and users can check on the status of the approval and provisioning processes. The different elements of identity management also mean the client is better able to meet government and industry PHI security regulations such as HIPAA and HITECH.

It has also reduced the number of access requests from 11,000 per month to a much more manageable number. Previously, if a person requested access to a particular application, eight people would have to approve it before IT could start provisioning. With the branded interface, the process requires only two approvals before provisioning.

When the project began in 2015, the client had 12 people performing identity management functions. Once the project is fully implemented, the company expects to require only four personnel for all identity management tasks, freeing the other eight to be reassigned to other, more value-added jobs.

Sirius helped the client consolidate four identity management systems into one user-friendly interface, saving on administrative costs and increasing efficiencies.

For more information about how the Sirius Security practice uses products from the IBM Security stack to protect organizations from external and internal threats, and achieve industry and government compliance, speak with your Sirius representative, visit www.siriuscom.com/security, or contact Sirius today.

SSTA_HEALTHSEC October 2017