precisely

Case Study:
Banque de Luxembourg

Overview

Banque de Luxembourg is one of the largest private banks in Luxembourg with multiple offices and total assets in excess of 12 Billion Euros. Originally founded in 1920, the bank has become a center of expertise in international finance offering a wide range of portfolio management solutions for its depositors and clients.

The bank was one of the early adopters of e-banking and developed a state of the art internet platform to provide access to account information, bank statements, and investment portfolios 24 hours a day, 7 days a week. The e-banking system quickly became a significant part of the overall banking operation and currently the bank supports more than 30,000 secure remote accesses per day.

Executives were committed to the expansion of services to remote depositors and clients and quickly recognized the need to adapt another level of security that would scale with these services in the years ahead.

Banque de Luxembourg put together a team of experts to evaluate the possibility of expanding their security framework to address two primary objectives:

- Allow the bank to more quickly expand their auditing capability to meet the increasing demands on their System i.
- I Offer a centralized approach to securely monitoring and managing user access to include a new breed of remote user interfaces (ODBC, FTP, TELNET, IFS, etc).

> “Our mission is to monitor and securely manage access to our banking platform; among all the tools evaluated, the combination of Assure Monitoring and Reporting and Assure System Access Manager is by far the most effective, the easiest to implement and set up, does not impact on machine resources and is the most customizable. Precisely’s ability to respond to our needs and problems is unequalled in both quality and speed of response. This tool has become very useful and necessary for us.”
>
> - René Chevremont, IT Security Manager

The Challenge

In addition to supporting more than 750 users across multiple countries, the sheer number of online transactions the bank supports on a daily and weekly basis presented a unique challenge for the internal IT staff. On any given day the amount of data captured within the journal receivers could exceed 15 Gigabytes for Database transactions and more than 5 Gigabytes for System events.

Any security solution the bank adapted to their in-house applications had to be capable of handling this level of activity without adversely effecting performance or increasing their online storage requirements.

Equally important was the need to develop a solution that would integrate seamlessly with the bank's internal HA systems and financial platforms. The bank currently uses ERI Bancaire's Olympic banking information system to manage all of the front office and back office operations and an HA solution from Precisely to routinely replicate all of their production systems.

Access to the banking applications was controlled largely through an older third party program. As the bank continued to expand the various services and general access to the System i, it was clear they needed to adapt a much more automated approach to managing user access. Beyond the traditional green screen access, the bank anticipated a requirement for incorporating a number of exit programs (FTP, DDM, ODBC, DRDA, etc) into their system. In addition to having the flexibility to adapt to these exit points, the final security solution also needed to incorporate a level of automation that would minimize the resources needed to support access points, authority levels and applications.

Scalability, performance, and compatibility were three of the most critical features the bank needed to incorporate into their overall security solution.

Solution

The executive team put together a prioritized list of requirements and spent a number of months evaluating several security vendors for their System i. A "Best of Breed" approach was considered early on, but the bank clearly understood the benefits of adapting a single platform if they could find a solution capable of meeting their complex auditing and system access requirements. After careful evaluation the bank selected Precisely's Assure Monitoring and Reporting as the solution for auditing and Assure System Access Manager for access control. Their decision was based on a number of criteria including:

- Assure Monitoring and Reporting's unique ability to audit events at both the system and database level.
- Impact on Sytem i Performance - Extensive testing was completed with several vendors and Assure Monitoring and Reporting and Assure System Access Manager had virtually no impact on overall system performance.
- Fully integrated Enterprise wide solution that included Assure System Access Manager for managing the System i exit programs.
- The ability to securely manage access to the System i through multiple protocols.
- Flexible Reporting Features - Assure Monitoring and Reporting offers an unlimited ability to schedule reports, alarms, e-mail alerts in a format that can be customized to meet the requirements of both the in-house staff and external auditors.

Results

The initial phase of the security system was fully implemented in less than two weeks and over the next two years the system was expanded, step by step, to include a significant number of perimeter systems and databases. The bank quickly made very effective use of Assure Monitoring and Reporting's ability to generate a variety of standard reports, customized reports for auditors, e-mails, and PDF files for general or limited distribution. Sensitive reports or events, for example, are limited to only those individuals that are part of the Governance Committee while other system reports are sent to the support group.

Assure System Access Manager was the second component the bank implemented as part of their security expansion. Today the solution manages access to any point into the System i and every event is logged, compressed and segregated into monthly logs and stored on line for a total of six months. Much like Assure Monitoring and Reporting, Assure System Access Manager has the ability to generate alarms based on specific events or even specific sensitive commands. The Security Director at the bank selectively creates alarms and triggers as part of their on-going policy development.

Over time Banque de Luxembourg expanded the functionality of Assure System Access Manager to include the SQL/QRY exit program. With the addition of the SQL Engine module the bank now has complete visibility of any access to production files using STRSQL, WRKQRY, RUNQRY, RUNSQLSTM, DRDA, etc. Although the process of effectively managing and controlling access through SQL can be process intensive, the solution has successfully managed this complex process with virtually no impact on overall system performance.

Conclusions

The reactions which followed the implementation of Assure Monitoring and Reporting and Assure System Access Manager have been very positive. Both internal and external auditors are pleased with the ability of the platform to generate concise and accurate reports. Equally important is the fact that today, the auditing and compliancy process is significantly more automated, eliminating the need for IT personnel to spend hours gathering system information, managing user access, and formatting the data into reports that the auditors can interpret.