CASE STUDY

LogRhythm Delivers Internal Auditing Requirements while Securing a Sophisticated Network

LogRhythm

FORTIS BANK

Organisation
Fortis Bank
Hong Kong Branch Office

Industry
Financial Services

Employees
Over 300

Challenges
- Each device and server type had unique log taxonomy making it difficult to provide meaningful reports
- Log data overwritten quickly if not exported to an external source
- Firewall logs manually backed up and reviewed

Benefits of Deployment
- Powerful, affordable platform
- High-quality, local support
- Built-in automation
- Simple, user-friendly interface
- Comprehensive compliance reporting
- Granular analysis of user behavior

> "LogRhythm's ability to handle huge amounts of log data, provide granular analysis of user behavior and comprehensive "out of the box" management reports...were all drivers to select LogRhythm."
>
> *David Wong*
> Network Administrator
> Information Technology
> Fortis Bank Hong Kong Branch Office

Fortis Bank has long been one of Europe's leading financial institutions, providing a broad range of banking services to personal, business and institutional customers around the globe. After joining with BNP Paribas in May of 2009, Fortis Bank is now a member organization of what Standard & Poor's has named as one of the six most solid banks worldwide. The organization has always practiced strong governance with an emphasis on best practices.

Business Requirement
As a part of Fortis Bank's institutional culture, internal auditors require that the IT Department take specific measures to improve information security and protect customer data. The auditors require that the IT department centrally collect and archive all log data, with the ability to both export it to tape for cold storage and to easily recover it for future use. A more specific policy mandates that user account maintenance is tracked and reviewed on a consistent basis by Fortis Bank's information security officers.

IT Environment
Fortis Bank Hong Kong Branch Office employs over 300 people at three separate geographic locations. The network is heterogeneous in nature, with a combination of Windows and Unix-based servers, and a variety of firewalls and network devices.

Technical Challenges
The heterogeneous nature of the network created a few difficulties for reviewing and reporting on log data:
- Each device and server type had its own log taxonomy making it difficult to sort through the data or provide meaningful reports.
- There was a limited retention period on Windows devices, meaning log data would be overwritten quickly if it wasn't exported to an external source.
- Firewall logs were being manually backed up and reviewed as necessary – a time-consuming and difficult process.

In order to fully comply with internal auditing requirements, Fortis Bank Hong Kong Branch Office required a log management solution that would safely collect all server and network device logs, translate the data into useful information, and automate the process of creating reports for the information security officers.

Solution
During the selection process Fortis Bank evaluated several enterprise log management platforms. Although several products were able to meet a few of their requirements, only LogRhythm was able to provide a cost-

effective solution that met all of Fortis Bank's needs as well as providing additional operational value. The comprehensive benefits combined with high-quality support services provided by a local partner made LogRhythm the obvious choice.

LogRhythm's centralized architecture and agentless collection capabilities make it a simple solution to implement and operate. Despite collecting log data from three locations, LogRhythm provides a simple interface for managing all log data through a single, user-friendly console. All data is automatically sent to a secure and centralized archive for long-term retention, with a wizard-based tool allowing simple and quick extraction as needed. Flexible architecture, with the means to securely and reliably transmit remote data, as well as a cost-effective, software-based deployment option made LogRhythm the best choice from an implementation standpoint.

> "LogRhythm's ability to handle huge amounts of log data, provide granular analysis of user behavior, offer comprehensive "out of the box" management reports, combined with LogRhythm's local partner's ability to provide high-quality professional services and support were all drivers to select LogRhythm."
>
> *David Wong*
> Network Administrator
> Information Technology
> Fortis Bank Hong Kong Branch Office

Built-in automation was another key requirement for Fortis Bank. LogRhythm provides automated data normalization, proactive event filtering, and the ability to generate and publish auditing report packages on a set schedule. Normalization presents Fortis Bank with valuable information translated from all of its different log sources in one consistent and easy-to-read format. LogRhythm also has built-in filtering that ensures Fortis Bank is able to focus on relevant event information without having to sift through large amounts of insignificant data. An additional feature allows users to easily create powerful Alarms that will automatically notify them of specific events while eliminating false positives before they are generated.

Conclusion

LogRhythm has automated the time-consuming process of collecting, filtering and archiving log data and generating useful reports for auditors at Fortis Bank Hong Kong Branch Office. It also provides valuable information to administrators for insider threat detection and proactive troubleshooting. By implementing LogRhythm, Fortis Bank not only satisfies internal auditing requirements, it also benefits from a powerful tool for daily use in securing and optimizing their network.