Case Study – A Fortune Global 500 Chinese Bank

Helping a bank to ensure compliance with regulatory requirements set by the Hong Kong Monetary Authority for safeguarding sensitive customer data

Client Profile

This is one of the largest banks in China, ranking among the Fortune Global 500 companies.

The Challenges

Banks possess a large amount of sensitive data, such as customer personal information, account records, financial status, credit ratings, and more. These data are stored in different systems within the bank, which are isolated on separate networks and equipped with multiple security measures. In general, when employees use these systems, their computers are not connected to external networks, ensuring a high level of security.

However, in practical operations, there are instances where certain colleagues need to send specific data to customers or other relevant institutions. In such cases, the data needs to be synchronized to a network that can communicate with the outside world (referred to as an "open network"). When employees access these data, their computers are able to send emails and access the internet. It is crucial to ensure that this sensitive information is properly used and not abused. However, if every instance of data transmission required approval from superiors, it would significantly impact work efficiency, and superiors would spend a considerable amount of time on approvals. Therefore, a solution is needed that provides adequate protection when employees access sensitive data, preventing data leakage. At the same time, when there is a need to send out these documents, a comprehensive record of the related operations should be maintained, making it easy for department management to track which documents were sent and the reasons behind them.

The Solution

In the end, this bank chose Curtain e-locker DLP system to protect the data synchronized to the open network. When employees access this data, it is controlled and protected by the software. However, employees are also given permission to send documents to customers or external institutions without requiring approval from superiors. When an employee copies a document outside the system, the software prompts them to fill out a form, requiring them to declare the reasons for the data transmission, whether it contains personal information, the quantity of data involved, etc. This information is uploaded to a database, and records are automatically sent to the relevant departments on a weekly basis for review and documentation.

This bank has been using the relevant solution for over five years. Due to the system's flexible permission settings, customers can choose different

Environment

Server-side:
- Windows File Server

Client-side:
- Windows 10 & 11

Application:
- Microsoft Office
- Adobe Acrobat Reader

Products

- Curtain e-locker Office Suite
- Curtain e-locker Protector for Windows File server

configurations and combinations. Curtain e-locker can effectively reduce the risk of data being misused and is aligned with actual workflow and business requirements. It also meets the bank's information security requirements and complies with relevant guidelines from the Hong Kong Monetary Authority.

The Results

- Effectively prevent unauthorized use of sensitive data
- Avoid excessive approval processes that may impact employees' normal work and efficiency while serving the purpose of review and investigation
- The system can automatically send declaration records to relevant department personnel based on the user's department affiliation.
- Meet internal and regulatory requirements for information security

For more information, please contact us.
Coworkshop Solutions Limited
General Enquiry: (852) 2776 6161
E-mail: info@coworkshop.com
Website: www.coworkshop.com
More case studies: www.coworkshop.com/CaseStudies