



Case Study – A Hong Kong Government Department

Helping this government department protect multiple systems to ensure that the relevant raw data and analytical results are not leaked when employees are conducting data analysis

Client Profile

This government department engages in extensive data collection and analysis to assist the government and various sectors of society in conducting relevant research, discussions, and planning.

The Challenges

This department places great emphasis on data security. Due to their frequent need to collect large amounts of data and perform analysis, much of the raw data may contain sensitive information, and the analytical results cannot be freely disclosed. They constantly remind employees to handle data and analytical results with caution. However, in an organization with thousands of employees, it is understandable that human errors can occur given the significant workload each day. In the past, there have been incidents where employees accidentally uploaded sensitive data to websites. Therefore, they are seeking a solution to ensure that sensitive data is not leaked and to minimize the associated risks.

Over the years, the department has acquired a range of systems and analytical tools to meet their practical needs, including FoxPro, SAS, and Tableau. Additionally, they have developed their own tools using programming languages like Python and R for various data analysis purposes. They are in need of a solution that can seamlessly support these diverse systems, platforms, and tools without introducing additional maintenance responsibilities to their daily operations.

The Solution

Eventually, this department decided to use Curtain e-locker DLP. The design of Curtain e-locker's protected zone is highly suitable for their needs. During data analysis, the raw data and analytical results typically do not need to be shared externally. The protected zone ensures that regular users cannot transfer data to email, external websites, USB devices, and similar devices when using the raw data for analysis. The system also enables employees to share controlled data within the company but only on department computers and within specific boundaries. If employees need to share this data externally, they must submit a request through the system and obtain approval from their superiors. This permission setting aligns well with their daily workflow and significantly enhances data security without hindering their work.

The department has been using this solution for over three years and is highly

Environment

Server-side:

- SAS Server
- Tableau Server
- SQL Server
- Windows File Server

Client-side:

- Windows 10 & 11

Application:

- Microsoft Office
- Adobe Acrobat Reader

Products

- Curtain e-locker Office Suite
- Curtain e-locker module for FoxPro, SAS, R, Python, T-ARGUS, SSMS, and Tableau



satisfied with it. They have also expanded the software's functionality to different analysis systems on multiple occasions.

The Results

- Ensuring that the raw data and analysis results are not leaked
- Avoiding data leaks caused by human errors
- Supporting different data analysis systems, platforms, and custom developed tools
- Simple system maintenance
- All actions and operations being logged for easy auditing purposes

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

