Case Study – A Hong Kong Government Department

Assist this government department in protecting an internal web system to ensure that data is not leaked when employees use the system

Client Profile

This is a department of the Hong Kong government that handles one of the main sources of government revenue.

The Challenges

This department has multiple internal systems, and one of them stores a large amount of confidential data. They need a solution to ensure that users of the system do not leak the data while using it.

While the department already has various security measures in place, they primarily focus on protecting against hackers, computer viruses, and external attacks. As for internal employees, especially authorized users of the system, they mainly rely on operational guidelines and employee discipline. However, in an organization with thousands of employees, it is difficult to guarantee that there won't be a few bad actors. Moreover, employees can make mistakes during their work, and it cannot be ensured that they won't accidentally leak sensitive data.

Therefore, they have explored some data leakage prevention solutions available in the market and found that most of them are based on keyword or data pattern scanning to identify and control confidential data. However, these solutions often rely on a scoring system where the more frequently certain keywords appear, the more likely the data is considered confidential. This approach can lead to a significant number of false positives, affecting normal employee operations.

The Solution

In the end, this department chose to use Curtain e-locker DLP. Curtain e-locker allows them to independently determine which systems need protection, without relying on keyword scanning. As a result, there are no false positives, and they can selectively protect certain systems without impacting normal user operations. Employees can continue to browse the internet, send emails, and use devices like USB drives. However, when using a protected system, their actions are limited based on their own permissions. If they do not have the authorization, they cannot transfer data to email, USB drives, and other devices. The solution also addresses finer details such as copying and pasting content to other locations, taking screenshots, and applying screen watermarks.

For special cases where regular employees need to send sensitive data, they

Environment

Server-side:
- Red Hat Web Server
- 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 Web Application
- Curtain e-locker Protector for Windows File server

can submit a request through the system. After approval from senior management, they can temporarily release the files. All actions are recorded by the system for audit purposes.

This department has been using this solution for over two years and is highly satisfied with its performance. They are considering implementing the solution in other internal systems that require similar protection.

The Results

- Targeted protection of systems that store confidential data
- No false positives that would disrupt normal employee operations
- Reduced reliance on employee discipline alone, as the system ensures better data protection
- All actions are logged by the system for easy auditing

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