Safeguarding School Data: Understanding Data Leakage and the Role of DLP

Hong Kong Institute of Information Technology
香港資訊科技學院
Member of VTC Group VTC 機構成員

Objective

- Understand what data leakage is and its risks in schools.
- Recognize real-world examples of data breaches in education.
- Learn the role of DLP in preventing data leakage.
- Explore strategies to implement DLP in schools effectively.

- Examples of sensitive data in schools:
  - PII - Student personal information (names, addresses, grades, medical records).
  - Academic related records
  - Staff information (payroll, contact details).
  - School financial data or operational plans.

- Data leakage refers to the unauthorized **transmission, access, or exposure** of sensitive information to unintended recipients.
- Examples:
  - Use of multiple platforms (e.g., web-based self-developed systems which may be vulnerable, and public cloud storage without proper access controls).
  - Storing student data in traditional ways (e.g., using Excel to store student records, which is portable and prone to unauthorized access).
  - Weak or shared passwords.
  - BYOD (Bring Your Own Device) policies and unsecured personal devices.
  - Targets of cyberattacks like phishing and ransomware.

- Example 1: Exam Paper
  - An exam paper stored as a **Word** file on a shared drive was copied by a teacher to their personal PC, which was left **unattended**. A **student used a USB drive to access and copy the paper without authorization**.

Root Causes

1.Weak Storage Practices:

1. Sensitive files placed on a shared drive without encryption.

2.Lack of Security Awareness:

1. Teacher copied the file to their **personal device** without encryption or additional safeguards.

3.Physical Security Negligence:

1. Teacher's PC was left unattended in a location accessible to students.

4.Unrestricted USB Access:

1. USB ports were not disabled or restricted, allowing unauthorized copying.

- Example 2: Poor Access Control on Shared Drives

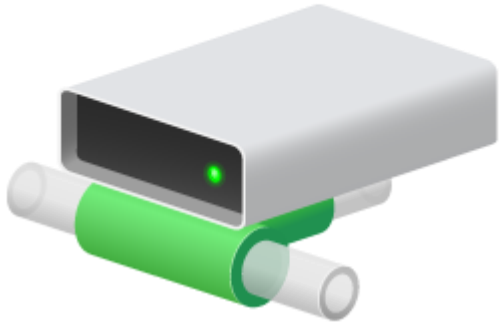
A school **shared drive with no access controls** allowed ransomware from a teacher's PC to spread, encrypting exam papers, student records, and files, causing data loss, disruption, and legal risks.

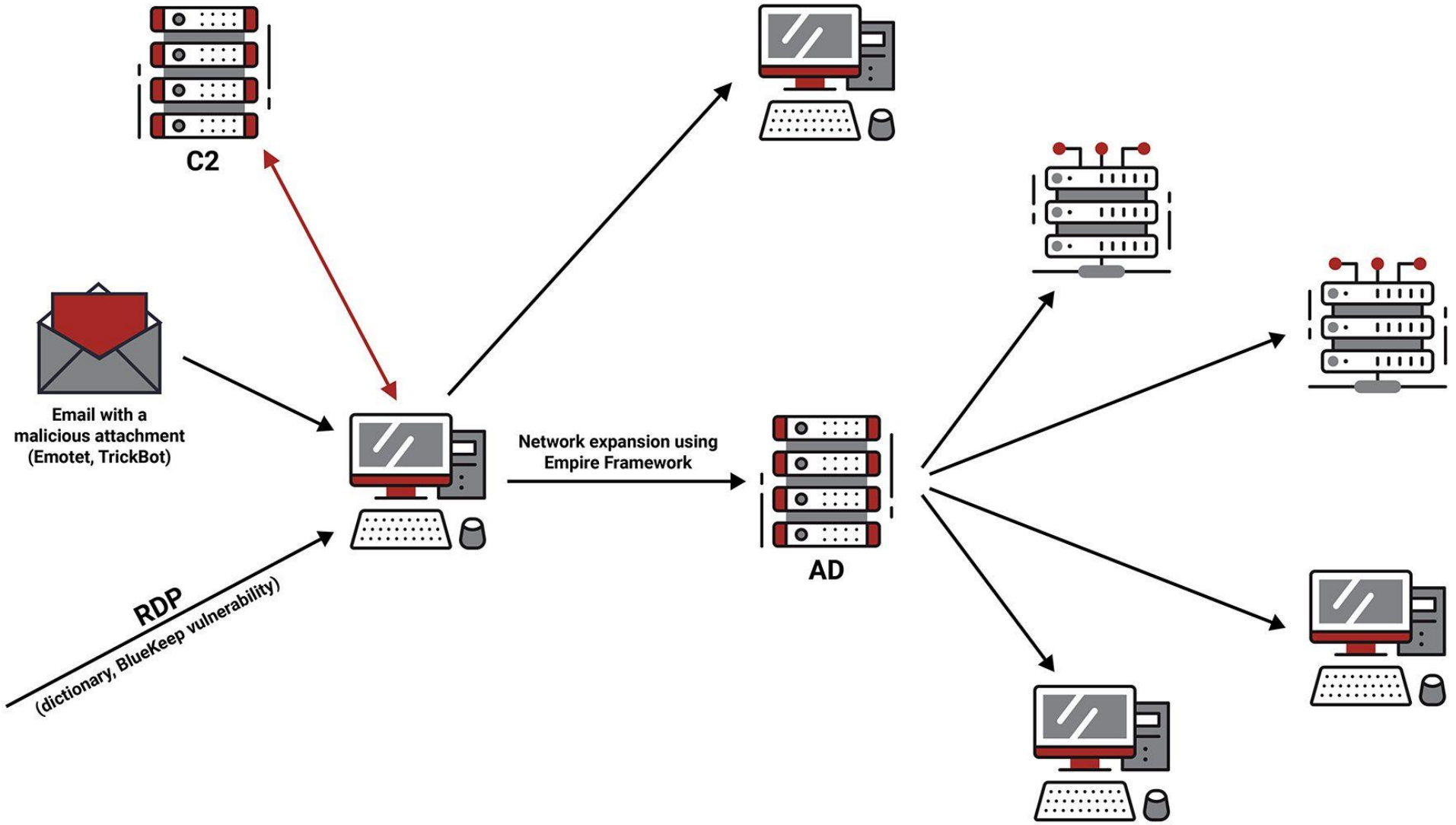
Shared Drive Setup:

- Connected to all teacher PCs.
- No proper access controls — unrestricted file access for all users.

Ransomware Attack:

- A teacher's PC was infected with ransomware.
- Malware spread through the shared drive.





https://security.geant.org/advanced-ransomware-attacks/

- Example 3: PII Storage in Traditional Methods

Paper records, unprotected files on shared drives, printed documents, or USB drives.

1. **Traditional Storage Methods:**
    1. Paper records, unprotected files on shared drives, printed documents, or USB drives.
2. **Key Issues:**
    1. **No Access Control:** No restrictions on who can view, copy, or access sensitive information.
    2. **Portable Risks:** Data can be easily printed, copied to USB drives, or taken out of the premises.

- Impact of Data Leakage
  - Loss of trust from parents, students, and staff.
  - Legal penalties for violating data protection laws (e.g., PCPD).
  - Financial costs of breach recovery.
  - Reputational damage.
  - Emotional distress for affected students and teachers.

Office of PCPD

- Office of the Privacy Commissioner for Personal Data, Hong Kong
- (個人資料私隱專員公署)
  - enforce the Personal Data (Privacy) Ordin
  - educate the public about personal data
  - moderate any dispute regarding person between two parties.

Office of PCPD (2)

- Additional roles of PCPD
  - Accept of a complaint from general publics
  - Exercise general powers of investigation
  - Issue an enforcement notice to offender(s) for amendment of violation
    - PCPD will take up legal actions if the offender(s) do not take action to improve
  - Provide legal assistance for civil claims

校園驗毒存保安漏洞

【本報訊】個人資料私隱專員公署昨就大埔區校園驗毒試行計劃發表視察報告，指出計劃下的資訊科技及通訊系統和裝置有保安漏洞，包括有兩間學校將儲存了學生個人資料的USB記憶體與寫有保護密碼的字條竟放在一起。公署向港府及相關單位提出十五項改善建議，包括港府應主動為同類計劃制訂一套資料保障政策及程序指引。

_5825_c.pdf)

[1] 發現的缺點包括：

(a) 一間被抽樣選中的學校有職員利用自己私人擁有的電腦處理參與學生的個人資料，但他們沒有獲提供保護個人資料的措施指引；

(b) 承辦商提供專用遙距伺服器，以隨機抽選學生接受快速測試及儲存測試結果。不過，禁毒處並沒有先小心評估聘用承辦商比由校外專責隊伍自行提供設施的好處。此外，沒有合約條文規定承辦商要提供安全措施以保障受託的個人資料；

(c) 校外專責隊伍並沒有遵從禁毒處的規定而採用SSL技術把傳輸進出遙距電腦的資料加密，及使用雙重身份驗證以控制用戶的使用權限；及

(d) 校外專責隊伍以USB記憶體儲存同意參與學生及被選中參與快速測試的學生的個人資料。USB記憶體然後被交給參與學校及計劃主任。雖然這些裝置均由密碼保護，但公署發現在兩間被抽樣選中的學校中，USB記憶體是與載有相關密碼的字條放在一起，因此使用密碼也是徒然。

https://orientaldaily.on.cc/cnt/news/20120727/00176_030.html

近年有關學校及非牟利機構的資料外洩事故呈上升趨勢

私隱專員公署留意到近年涉及學校及非牟利機構的資料外洩事故呈明顯的上升趨勢。2023年，公署接獲的157宗資料外洩事故通報當中，學校及非牟利機構的個案共61宗（佔整體個案約39%），比2022年的25宗（佔整體個案約24%）上升接近一倍半（140%）。2024年首三季，公署共接獲51宗來自學校及非牟利機構的資料外洩事故通報，佔整體個案總數約33%，與上年同期接獲此類個案的百分比相若。因此，私隱專員認為學校及非牟利機構不能掉以輕心，應投放足夠資源以提升資料保安措施，從而減低個人資料系統遭受網絡攻擊的風險。

私隱專員公署2022年至2024年（截至9月）接獲涉及學校及非牟利機構的資料外洩事故通報的統計數字如下：

年份	學校及非牟利機構的資料外洩事故通報宗數（百分比）	資料外洩事故通報總數
2022	25（約24%）	105
2023	61（約39%）	157
2024（截至9月）	51（約33%）	155

Is it too far from you? Try it yourself!

Search in Google :

1. filetype:xlsx passwords
2. intitle:"index of" "backup.zip"

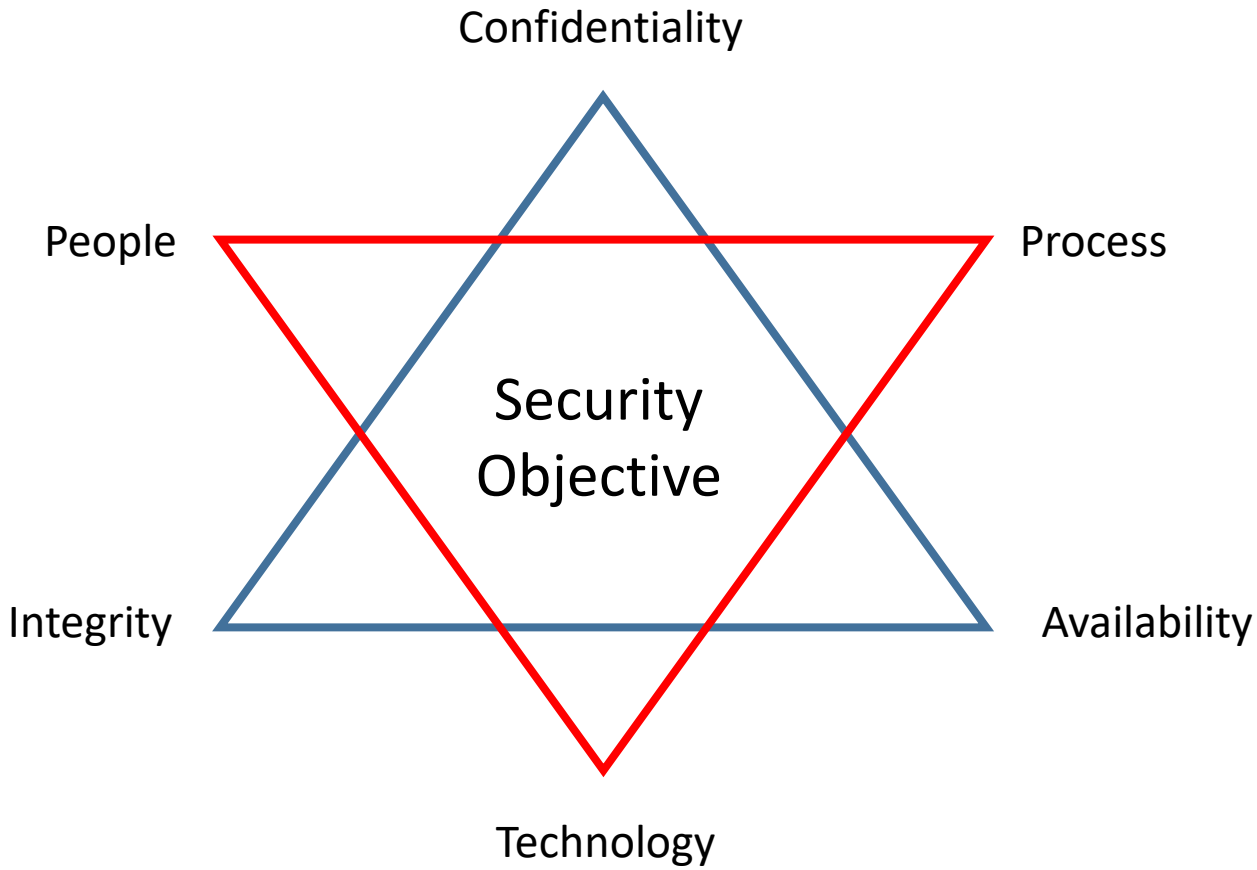
References : https://www.exploit-db.com/google-hacking-database

There are too many ways to leak data out…

- **Print**
- **Print screen**
- **Save to USB disk**
- **Copy & paste**
- **Email**
- **WhatsApp, Skype, WeChat**
- **Upload to Dropbox, FTP**
- **Take video by cell phone**
- **More…**

Gmail Outlook

Foundation of Information Security



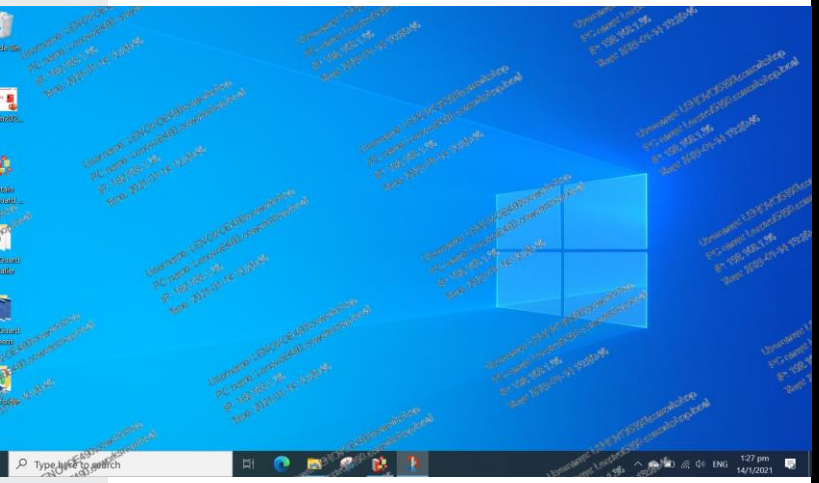
- **What is Access Control?**

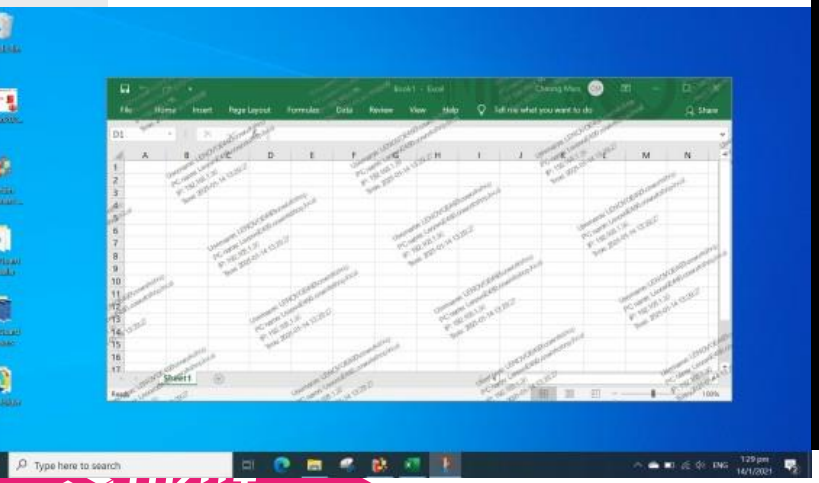
1. Who Can See What
   - Only the right people (e.g., teachers, principals) can see certain information, like student grades or exam papers.
2. Who Can Do What
   - Limits what actions people can take, such as editing records, sharing files, or printing documents.
3. Separate Areas for Everyone
   - Students, teachers, and office staff each have their own "work areas" with access only to files they need.
4. Accountability
   - Tracks who accessed or changed information, so if something goes wrong, you know who was responsible.
5. Stops Mistakes
   - Prevents sensitive information from being accidentally seen or changed by the wrong person.
6. Prevents Data Leaks
   - Stops files from being shared, copied, or printed without proper approval.

- DLP in Action: Real-World Examples
  - Automatically encrypting sensitive emails.
  - Blocking unauthorized USB devices.
  - Preventing the sharing of documents containing sensitive information.
  - Monitoring file uploads to cloud services.

Free DLP Products - Curtain MonGuard

Displays a watermark with user info to discourage unauthorized screenshots or sharing.





Free DLP Products - Curtain LogTrace

- Tracing Create, Copy, Move, Print, Delete, Rename, Save, Close files
- Report for copying files to USB / insert USB

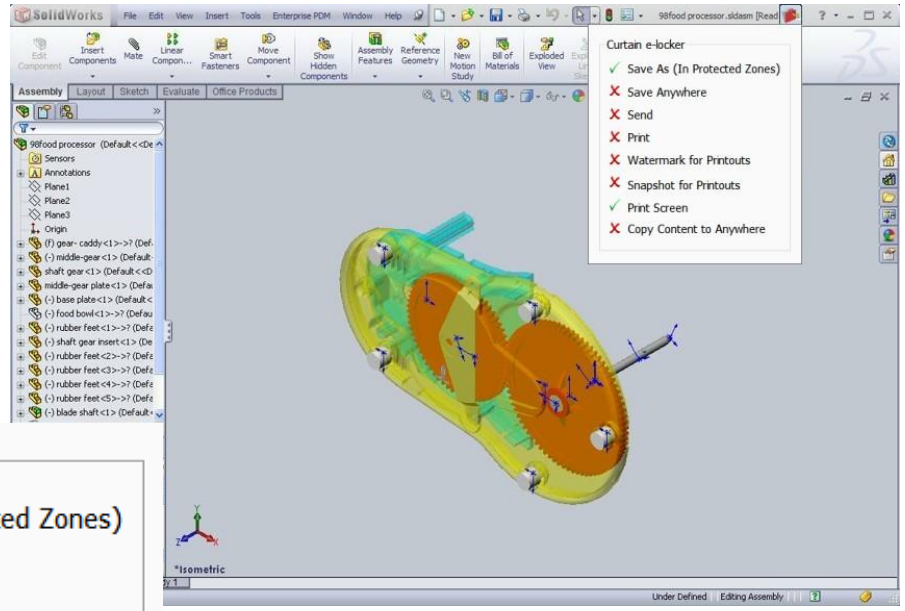
Curtain LogTrace

DLP with more features(cont.)

Curtain e-locker (DLP)

Data Loss Prevention

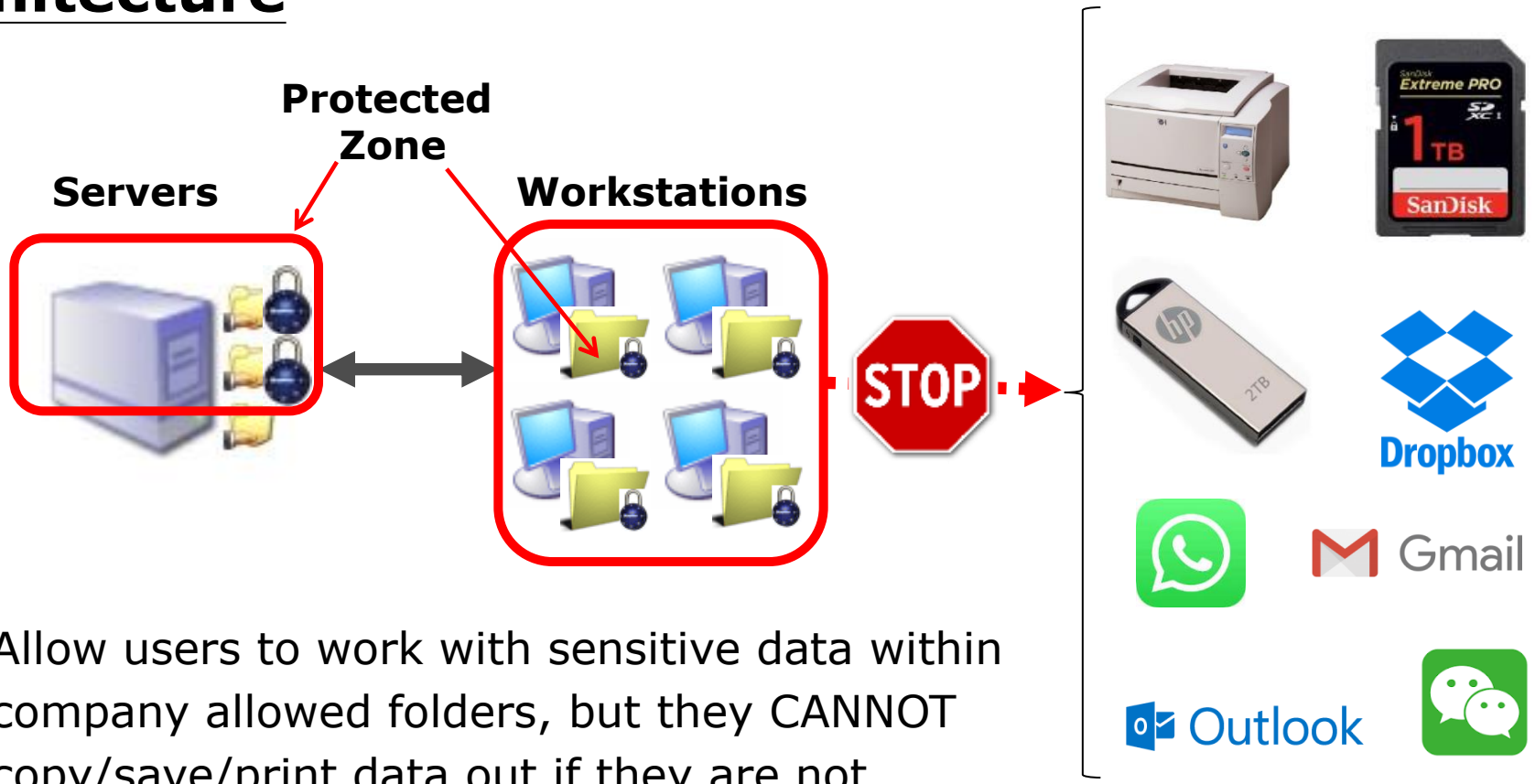
Control internal users



Curtain e-locker

- ✓ Save As (In Protected Zones)
- ✗ Save Anywhere
- ✗ Send
- ✗ Print
- ✗ Watermark for Printouts
- ✗ Snapshot for Printouts
- ✗ Print Screen
- ✗ Copy Content to Anywhere

Architecture



- Allow users to work with sensitive data within company allowed folders, but they CANNOT copy/save/print data out if they are not authorized to do so
- File / Print / USB log
- Support different systems (such as CRM, ERP, CCTV)

DLP with more features(cont.)
Zone-base DLP

e-locker DLP

Data Loss Prevention

File Rights:

- control **Save Anywhere**
- control **Send**
- control **Print**
- control **Print Screen**
- control **Copy and Paste out**
- control **New Document**

DEMO

Copy Restrictions:
•Copying is disabled, and the copy button cannot be clicked.

Watermark:
- Go to the settings page to configure the watermark for the application.

Local Download:
- Compare features for Account A and Account B on the settings page.

PrintScreen Protection:
- Open print screen tools.
- Show how files protected by eLocker are secure, compared to normal files.

Access Logs
- Audit log tail

- Request for Evaluation (Free Limited Trial License)

  https://docs.google.com/forms/d/e/1FAIpQLSfCIEpC0QKmc-hbZzwN6z1siz4bguNLVQO7FjsWaYMa_dP7jg/viewform?usp=sharing

Nicole Wu 2851 0271
nicolewu@udshk.com

Q&A