Data Loss Prevention

(Designs / Use Cases and Implementations)

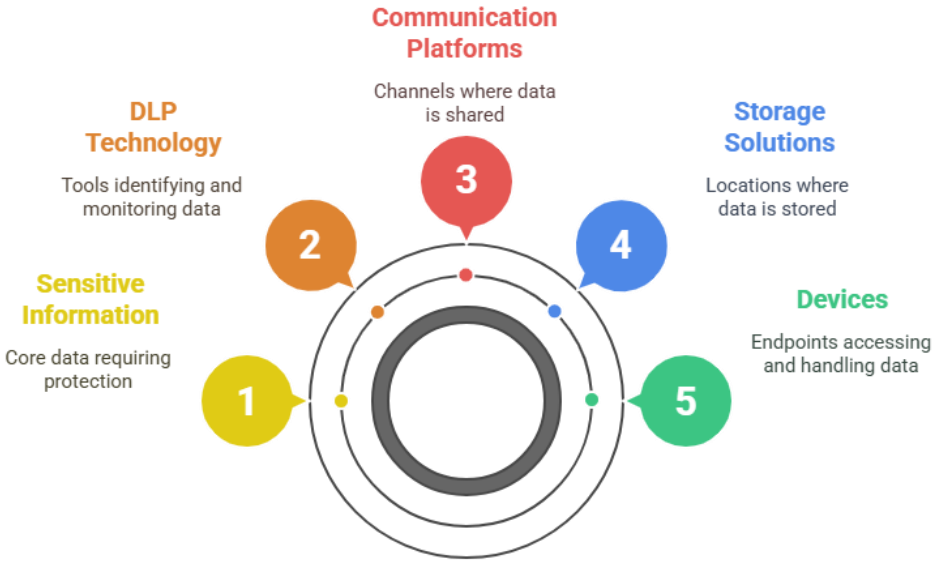
examlabpractice.com

What DLP Does

What DLP Does:

DLP identifies and monitors sensitive information—like credit card numbers, Social Security numbers, health records, or custom business data—across:

- **Emails** in Exchange Online
- **Files and folders** in SharePoint Online and OneDrive
- **Chats and files** in Microsoft Teams
- **Devices** if onboarded through Endpoint DLP



Design Use Cases for DLP

Regulatory Compliance Use Cases

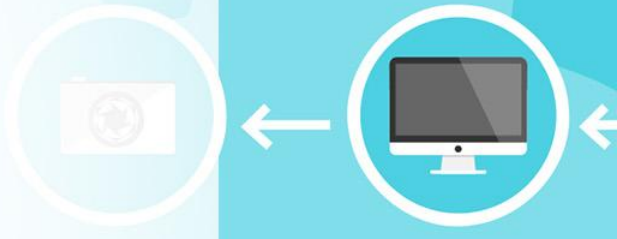
1. **Prevent exposure of credit card numbers (PCI-DSS)**
   - Block sharing of documents or emails containing credit card numbers outside the organization.
2. **Protect healthcare data (HIPAA)**
   - Detect and prevent sharing of documents with medical terms or patient information via email or Teams.
3. **Safeguard national ID numbers (e.g., SSNs, NINs)**
   - Alert or block emails and file uploads containing Social Security or tax ID numbers.

Internal Corporate Policy Use Cases

4. **Prevent accidental sharing of financial reports**
   - Block non-CFO employees from sharing quarterly results stored in SharePoint Online.
5. **Protect executive communications**
   - Apply stricter controls to email communications and files shared by board members or executives.
6. **Restrict upload of sensitive data to personal cloud storage**
   - Use Endpoint DLP to block users from uploading confidential documents to Dropbox or Google Drive.

Geographic or Business Unit-Specific Use Cases

7. **Block sensitive data sharing from EU users to non-GDPR countries**
   - Identify and prevent data transfer violations for GDPR compliance.
8. **Apply stricter policies to HR and Legal departments**
   - Ensure only authorized users can access and share contracts or employee records.



Design Use Cases for DLP (continued)

Device and Endpoint Use Cases

9. **Block copying of sensitive files to USB drives**
   - Prevent exfiltration via removable storage on managed endpoints.
10. **Prevent printing of confidential content**
    - Stop users from printing documents containing internal project code names or financial forecasts.
11. **Detect screen capture attempts**
    - Monitor or block screenshots of documents tagged with a sensitivity label (if integrated with sensitivity labeling).

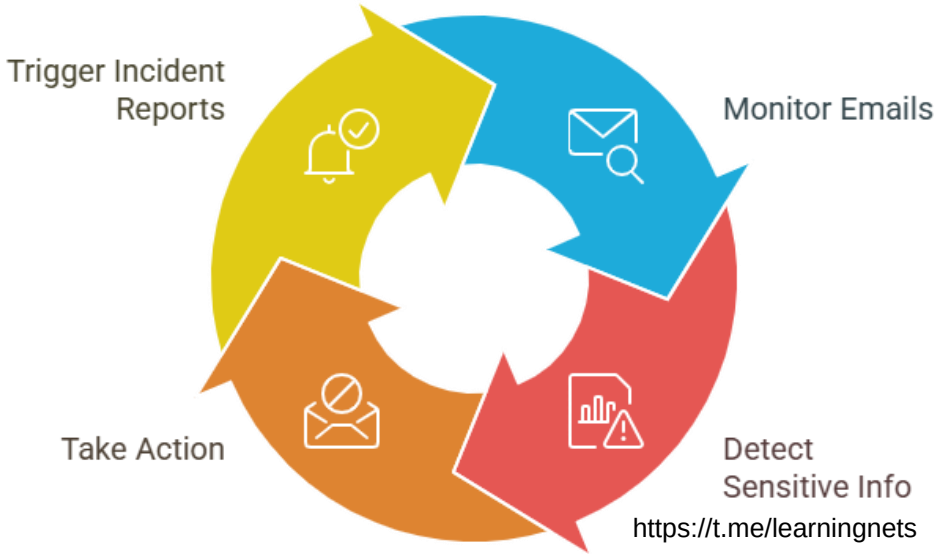
Communication Oversight Use Cases

12. **Stop external sharing of NDA-protected content**
    - Apply policy that detects keywords and phrases from NDAs and blocks emails or file sharing.
13. **Alert users before sending sensitive data**
    - Use policy tips in Outlook or Teams to educate users and reduce false positives.

Custom or Industry-Specific Use Cases

14. **Protect engineering schematics or CAD files**
    - Use custom sensitive info types or keywords to block unauthorized sharing of proprietary designs.
15. **Monitor legal case files**
    - Create a custom policy that flags names of active legal matters stored in SharePoint libraries.
16. **Detect internal leaks of source code**
    - Block attempts to copy/paste or upload code files from engineering laptops using Endpoint DLP.

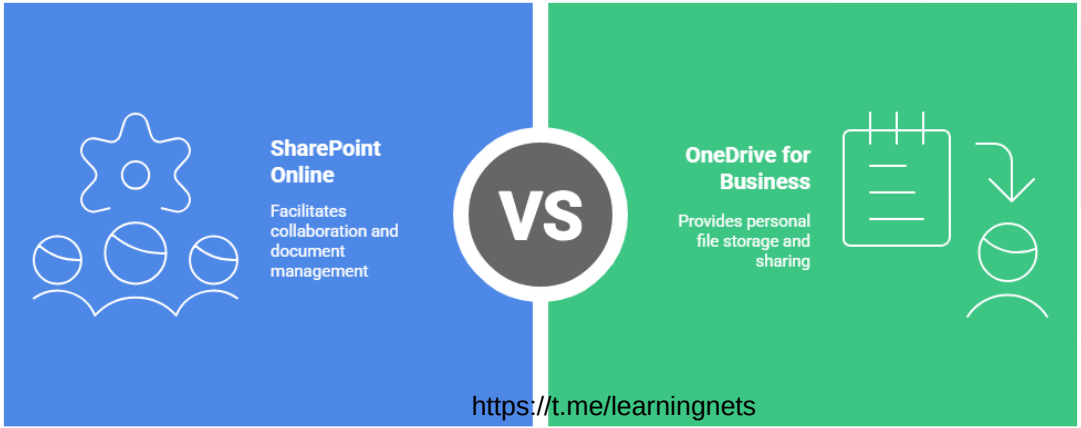
DLP with Emails in Exchange Online



- **Monitors email messages and attachments in real time.**
- **Detects when users try to send sensitive info (e.g., credit card numbers, financial data) externally or to unauthorized users.**
  - **Can: Block or encrypt the email.**
  - **Send policy tips to warn the sender.**
  - **Trigger incident reports to admins.**
- **Trigger incident reports to admins.**

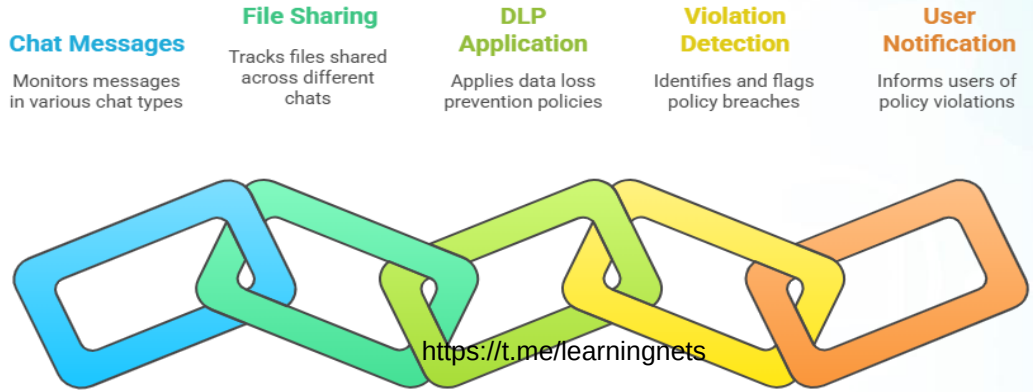
DLP with Files and Folders in SharePoint Online and OneDrive

- Scans files stored or shared in **SharePoint sites** and **OneDrive for Business** accounts.
- Detects sensitive content like **PII, financial, or health data**.
- Policies can:
  - **Restrict sharing** with people outside your organization.
  - Automatically **block download or access**.
  - Alert users with policy tips in Office apps (Word, Excel, PowerPoint).
- Works whether the file is actively being shared or just sitting in storage.



DLP with Chats and Files in Microsoft Teams

- Monitors **chat messages** and **files shared in 1:1, group, and channel chats**.
- Helps prevent accidental or intentional leakage of sensitive info (like sending a payroll document to the wrong team).
- DLP applies to messages sent through:
  - Teams desktop and web clients.
  - Mobile app (for supported features).
- If a violation is detected:
  - Message can be **blocked** from sending.
  - A **notification** is shown to the user (policy tip).



Devices (via Endpoint DLP)

- Extends DLP protection to **Windows client devices** onboarded through Microsoft Defender for Endpoint.
- Monitors **actions taken on files containing sensitive data**:
  - Copying to USB drives
  - Printing
  - Uploading to personal cloud apps
  - Copy/paste to unauthorized apps
- Can **block, audit, or warn** depending on policy.
- Adds visibility and control even **before data leaves the device**, complementing cloud-based DLP.