10.2.2 DLP Facts

Every business has sensitive data in its system and keeping it protected is a high priority. Data leakage happens when sensitive data like credit card numbers, intellectual property, financial information, or proprietary company information is disclosed to an unauthorized person. This lesson will look at five approaches to data security, including data loss prevention, masking, encryption, tokenization, and rights management.

This lesson covers the following topics:

- DLP
- Masking
- Encryption
- Tokenization
- Rights management

DLP

Data loss prevention (DLP) is a system that attempts to detect and stop breaches of sensitive data within an organization. Sensitive data is monitored by the DLP system in four different states:

- While in use on endpoint systems
- While in motion as it is transmitted over the network
- While at rest on a storage medium
- While being transmitted to or from cloud-based systems

Accordingly, there are many ways in which DLP can be implemented. Be familiar with the following:

DLP Implementation	Description
Network DLP	- A software or hardware solution that is typically installed near the network perimeter - Analyzes network traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies
Endpoint DLP	- Runs on end-user workstations and servers - Also referred to as a Chinese Wall solution - Could be something as simple as restricting the use of USB devices
File-Level DLP	- Used to identify sensitive files in a file system - Embeds the organization's security policy within the file - Travels with the file when it is moved or copied
Cloud DLP	- Software solution that is typically on cloud-based systems - Analyzes traffic to and from cloud systems in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies

Masking

Masking works by replacing sensitive data with realistic fictional data. There are different types of masking.

Masking Type	Description
Dynamic data masking	- Replaces original information with a mask that mimics the original in form and function, making it useful for data which is in use or processing. For example, someone's name would be replaced with another random name, or credit card numbers would be replaced with a random number that contains the same number of characters - Can be used to control which users can see the actual data - Original data can be retrieved
Static data masking	- Helpful for data at rest in a database and can be specified by field or columns - Good to use when making copies of a database for testing, development, or reporting - Original data is made irretrievable through reverse-engineering. A mask copy is made rather than masking the original database

Encryption

Encryption is an essential tool in data loss prevention specifically for data in motion and at rest.

- Happens when plaintext data is changed through an algorithm into unreadable ciphertext
- The encryption algorithm has a variable that is called a key
- The authorized user that receives the encrypted data can decrypt it through the cipher key

Tokenization

Tokenization is another effective tool in data loss prevention. Tokenization does the following:

- Replaces actual data with a randomly generated alphanumeric character set called a token
- Stores original data on a server
- Protects data on its server with authentication and authorization protocols
- Allows authorization only when correct token is presented

Rights Management

Another data protection tool is rights management.

- Data is protected at the file level
- Identifies sensitive files and embeds them with your security policies
- Security policy travels with the specific file, even when copied or moved
- Allows continued control access to the file even when it's no longer in your system

Rights management has two categories:

Rights Management Category	Description
Digital rights management (DRM)	- File-level management applied to rich media like music, videos, and software that are sold to consumers

	▪ Utilizes security technologies ▪ encryption ▪ permissions ▪ product keys ▪ limited install applications ▪ persistent online authentication to prevent: ▪ editing ▪ sharing ▪ unauthorized copying
Information rights management (IRM)	▪ Sometimes called enterprise rights management ▪ Focused on business-to-business file transfers such as: ▪ documents ▪ spreadsheets ▪ financial data ▪ emails ▪ Utilizes encryption and permissions to create rules for files to allow or deny: ▪ copying and pasting ▪ editing ▪ forwarding ▪ printing of documents