What is DLP? Top Popular DLP Tools and Technologies

DLP (Data Loss Prevention) is a set of solutions, strategies, processes, and technologies to protect sensitive data from being lost, stolen, accessed without authorization, or misused.

One of the technologies used to detect, prevent and protect data from loss or leakage in many businesses today is DLP. So what is DLP? What types of DLP techniques are being applied? Let's find out with ***TipsMake*** in the article below.

What is DLP?

DLP (Data Loss Prevention) is a set of solutions, strategies, processes, and technologies that protect sensitive data from being lost, stolen, accessed without authorization, or misused. DLP helps businesses protect data by monitoring, detecting, and preventing data transmission activities.

What is DLP?

How does DLP work?

The DLP operating process includes the following 5 main steps:

Step 1: Identify sensitive data

Businesses identify sensitive information that needs special protection. For example, personal information, intellectual property data, medical and educational data, financial information such as account numbers, CVV codes on bank cards, etc.

Step 2: Data monitoring

Once the data that needs to be protected is identified, DLP will scan all the data, including examining data traffic, monitoring accesses, and tracking user actions with the data.

Step 3: Detect danger

Based on rules, policies, and models, DLP evaluates activities such as accessing, copying, moving, or sharing protected data as threat behavior.

Step 4: Warning and prevention

When DLP detects threatening behavior, it alerts and prevents it. For example, it blocks sending or downloading data, encrypts data so that only authorized users can read it, and sends alerts to administrators about threatening behavior.

Step 5: Reporting and monitoring

DLP operates 24/7, recording all activities related to sensitive data and then providing detailed reports on data activities. Through this, businesses will better understand threats and promptly come up with better data protection measures in the future.

The Importance of DLP

Data is an extremely important asset for any organization or business. They directly determine the business activities and development of organizations and businesses. If a business loses data, its operations will be interrupted, even bankrupt.

According to IBM's latest Cost of a Data Breach Report, the average cost of a data breach increased 10% year-over-year to $4.88 million, the highest increase since Covid 19.

Personal information is valuable and often targeted by attackers. Half of all data breaches involved personal customer information such as tax, email, phone number, and address. Intellectual property (IP) records ranked second, accounting for 43%.

Data protection is becoming more urgent and difficult as businesses now store data in multiple formats and locations. DLP policies and tools help businesses protect data online in three states:

1. Data in use
2. Data in motion
3. Static data.

DLP acts as a monitoring system, continuously monitoring, reviewing and analyzing data to detect anomalies, preventing potential hazards and risks.

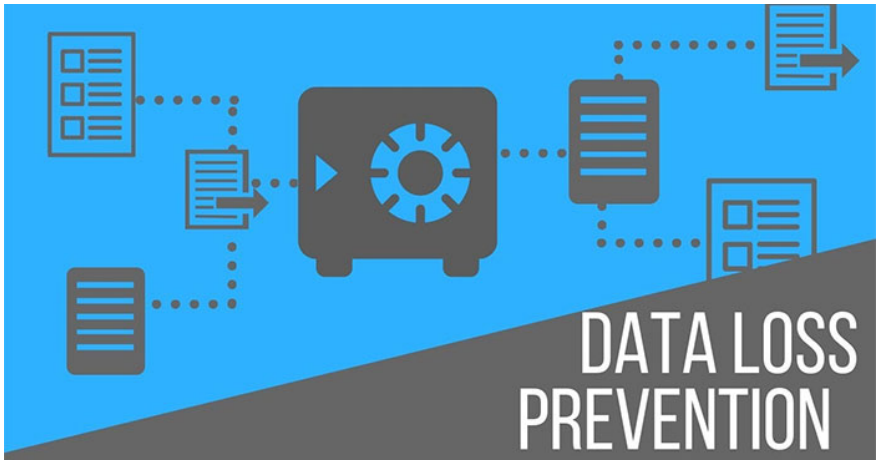
What are the common types of DLP techniques?

1. **Endpoint DLP:** Endpoint-based DLP monitors 24/7, protects data on all devices, strictly controls data copying and transmission activities, and prevents unauthorized intrusions.

2. **Network DLP:** Network DLP will monitor the entire network, prevent data leakage, detect and prevent unauthorized access and data misuse.
3. **Discovery DLP:** Discovery DLP is responsible for finding, classifying sensitive data, identifying security vulnerabilities and promptly handling them before they are exploited by bad guys.
4. **Cloud DLP:** Cloud DLP is responsible for protecting data security in the cloud, strictly controlling access, usage and sharing of data in the cloud.

Why choose to use DLP?

DLP is a solution that helps protect sensitive business data from theft, leakage and unauthorized access. According to Gartner's 2022 research, up to 35% of businesses do not deploy DLP solutions. As a result, they have to pay fines, be responsible before the law, affecting the reputation and revenue of the business. Therefore, using DLP is essential to:



Why choose to use DLP?

1. Protect sensitive data from theft, leakage, unauthorized access, misuse, giving businesses more time to focus on business development.
2. Comply with legal regulations on data security.
3. Demonstrate professionalism and prestige, enhance image and trust in the eyes of customers, attract more potential customers.
4. Optimize data management processes, save time and costs by eliminating the need to deal with data security issues.
5. Develop management policies to protect intellectual property rights or proprietary information of the business.
6. Compensate for the lack of experienced security professionals.
7. Protect your cloud, endpoints, and third-party tools from Ransomware attacks or other security threats.

Key elements to support DLP implementation

When implementing DLP strategies, to ensure effectiveness, you need to pay attention to the following factors:

1. Use 3rd party DLP vendors to test and validate data issues.

2. Use Framework to classify data (structured data, unstructured data, personal information, financial information, intellectual property data,.)
3. Set up precise data processing and correction to make management easier.
4. Deploy only one DLP strategy across different business units so that data is managed consistently.
5. Train staff on DLP policies and DLP security procedures

Popular DLP tools and technologies

In the market, DLP is divided into two main versions: dedicated and integrated:

1. **Dedicated DLP** : Dedicated, specialized, complex software products.
2. **Integrated DLP:** Integrates with a variety of security tools, lower cost of ownership than dedicated DLP.

Relying solely on conventional DLP solutions, businesses may face sophisticated attacks that cannot be detected, so businesses should apply additional third-party tools such as:

1. Broadcom Symantec Data Loss Prevention
2. Check Point Data Loss
3. CoSoSys Endpoint Protector
4. ManageEngine Device Control Plus
5. McAfee Total Protection for DLP
6. SolarWinds Data Loss Prevention with Access Rights Manager
7. Viking Cloud Endpoint Protection

Conclude

Implementing DLP is no easy task, but with careful preparation and the right tools, organizations can create a secure environment for their data. Remember, data security is not just the responsibility of the IT department, but of everyone in the organization.

You finished reading the article "**What is DLP? Top Popular DLP Tools and Technologies**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.