DATA LOSS PREVENTION (DLP)

What You Should Know

DLP simply means Data Loss Prevention.

DLP tools are basically security guards for your company's confidential data. They watch what data is going out and prevent leaks, accidental or intentional.

Data loss prevention is a set of technologies and processes that helps an organization enforce information handling policies and procedures to prevent data loss and theft.

DLP tools search systems for stores of sensitive information that might be unsecured, and they monitor network traffic for potential attempts to get sensitive information from the organization.

They help prevent sensitive data from being leaked, stolen, or misused by monitoring data in motion, at rest, and in use. DLP tools can also alert you of any suspicious or abnormal data activity, such as unauthorized copying, emailing, printing, or sharing of sensitive information.

DLP tools work by scanning and analyzing data in different locations.

They scan and analyze data in use, in motion, and at rest, identifying breaches of security policies. DLPs are often configured based on what an organization defines as sensitive data, thereby preventing such sensitive data from being shared.

Based on the DLP configurations, if the solution detects unauthorized actions, like copying or sharing of sensitive information, it responds by alerting administrators, encrypting data, or blocking actions to prevent potential data loss.

DLP tools continuously monitor data usage and user activities across networks, and endpoints in real-time.

When selecting the right DLP tools for your business, think data first; what you have and need to protect. There are several factors to consider, such as your data protection goals, data environment, compliance requirements and user experience.

Focus on getting a DLP solution that excels in data discovery, has data security features, and aligns with your organization’s budget. Ensure the tool integrates well with your systems, scales with your needs, supports compliance, and offers strong vendor support. It should be able to see how data is moving everywhere, through emails, and other messaging technologies to ensure there is no data leakage.

To get the most out of your DLP tools, start by developing a data protection strategy. Then align the policies and rules with compliance requirements. Ensure the DLP tools are compatible with your existing data environment and security solutions. Configure them according to your policies and rules, monitor them regularly, adjust as needed, then review and update them.

Educate your users on the benefits of DLP tools, provide training and support to help them understand how to use them correctly and the benefits attached.