Data Loss Prevention (DLP)

Return to Glossary

Data Loss Prevention (DLP) or **Data Leak Prevention**, **Information Loss Prevention** and **Extrusion Prevention** is a strategy for preventing individuals from accessing sensitive information who do not need it. It also ensures that employees do not send sensitive or critical information outside the corporate network.

While security teams use DLP to prevent sensitive information and intellectual property from leaking outside of the corporate firewalls, it's also a software strategy. And DLP use is growing. Gartner estimates that by the end of 2021, 90% of organizations will have implemented at least one form of integrated DLP, up from 50% in 2017.

There are two types of DLP products:

- Dedicated are standalone products, which are in-depth and complex
- Integrated products are more basic and work with other security tools.

These DLP products focus on policy enforcement and are less expensive than dedicated DLP tools.

DLP software products use business rules to enforce regulatory compliance and classify and protect confidential and critical information so unauthorized users cannot accidentally or maliciously share data that could put the organization at risk.

Sensitive information can be deliberately leaked or stolen by a malicious insider or external hackers, but research shows that most data loss is through internal staff making a mistake with no malice aforethought. However, that doesn't lessen the severity of the problem.

Source: https://whatis.techtarget.com/definition/data-loss-prevention-DLP