



What is Data Loss Prevention – DLP

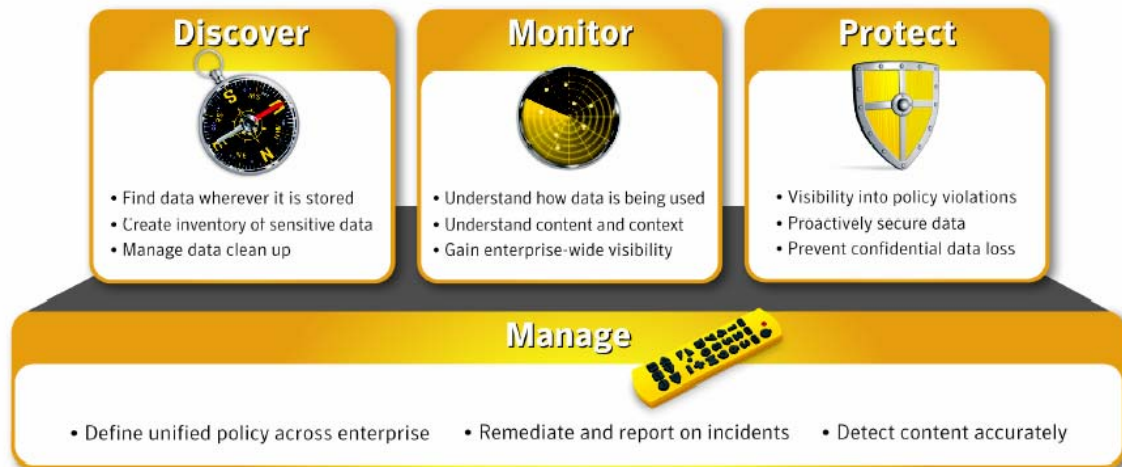
DLP is a process which helps the customers to accurately identify or discover, monitor, prevent and protect their confidential data from being misused knowingly or unknowingly by the employees. DLP is not about how you secure the data, but how well can we manage the sensitive data.

Data can be classified based on,

1. Data at Rest i.e. Databases, File Servers, NAS/SAN, Web Servers etc,
2. Data in Motion which is basically the Network and
3. Data in Use which is typically the Desktops and Laptops.

Why do Customer's require DLP

Data Loss Prevention delivers a unified solution to discover, monitor, and protect confidential data wherever it is stored or used. DLP offers comprehensive coverage of confidential data across endpoint, network, and storage systems—whether the users are on or off the corporate network. By measurably reducing risk, DLP gives organizations new confidence to demonstrate compliance while protecting their customers, brand, and intellectual property.



Must have Deliverables of a DLP solution:

1. **Visibility** : A true DLP solution should be able to discover the DATA regardless of whether its in a Network, Storage, Servers, Databases, Endpoints – On & Off the Network. By discovering the data customer finds it easy to identify where his/her sensitive data resides and how it can be taken care of.
2. **Risk Based**: A true DLP solution should be able to tell the customer when any sensitive data is tried to leak out of the network and the risk associated with this. Risk includes violation of any Regulatory compliance eg: HIPAA, GLBA,PCI etc by which this affects on the company’s Brand and Intellectual Property.
3. **Content Aware**: A true DLP solution can classify the sensitive data to 3 categories, **Structured Data** eg: Database, **Unstructured Data** eg: Web page , and an **Intellectual Property** eg: Mergers and Acquisitions, Pricelists, Source codes etc. By providing this information it makes easy for the customer to protect these sensitive data with policies and response actions incase of violations.
4. **Response to Threat in real time**: DLP solution should have an automated policy and responses to the real time threats by which it helps the organizations in performing a risk management and to make sure they do not violate any regulatory compliance.

5. **Work Flow Driven:** DLP solution is used to educate the customer and its employees that the company adheres to certain compliances and the entire team has to cope up with it. What we mean by Work flow driven is that, DLP solutions have a Top- Down management or vice versa, approach through which the response teams is correctly selected for any violations. Also DLP solutions will have an automated response to each and every incident happening inside the organization.
6. **Reporting:** This is one of the critical element of a DLP solution as it provides a deep insight in to the incidents occurred, which includes the employee who has violated the policies, through which means etc and using Snapshots to provide a complete evidence for the incidents.
7. And finally a DLP solution should be **Able to close the gap between people, policy and the technologies.**

Summary:

Data Loss Prevention delivers a unified solution to discover, monitor, and protect confidential data wherever it is stored or used. DLP offers comprehensive coverage of confidential data across endpoint, network, and storage systems—whether the users are on or off the corporate network. By measurably reducing risk, DLP gives organizations new confidence to demonstrate compliance while protecting their customers, brand, and intellectual property.

Protect	Brand & Reputation Customer and employee loyalty
Demonstrate	Regulatory Compliance Data Security best Practices
Reduces	Likelihood & Cost of Data leakage Competitive advantages due to loss of IP