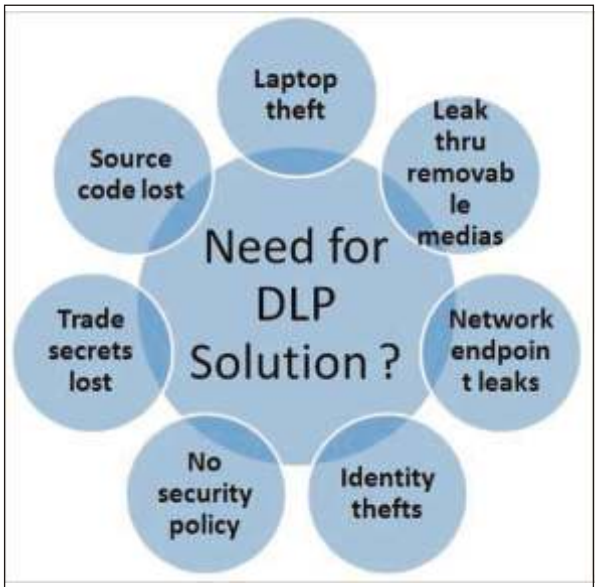
Data Leakage and Prevention Solution- The Next "big thing" in Security

Data Loss Prevention is one of the most hyped, and least understood, tools in the security space. In spite of the availability of many technologies, it can be difficult to understand the ultimate value of the tools and products best suited to the given problem. This report will provide the necessary background in DLP to help you understand the technology, know what to look for in a product, and find the best match for your organization.

V S Raghunathan
Senior Technichal Director
raghunathan.vs@nic.in

The need to protect key information assets in a wide open online environment has given rise to increasing demand for Data Leakage Prevention (DLP) solutions. The growing outsourcing business, distributed centres combined with intelligent hackers and identity thefts places government in greater risk. The data in e-governance applications are getting centralised at the SDC's and connectivity to the data is extended through State WAN where data leakage is becoming a serious problem.



Venn Diagram showing " Need for DLP Solution"

Applications like e-Office and paperless solutions wherein the entire file including the high priority and confidential files are digitally stored become vulnerable and any leakage is an alarming situation. The trust on the system is being questioned and this is one of the key challenges to the solution providers today. Central and State Governments are beginning to realise that their networks contain high-value sensitive data and information such as financial approval files, planning documents, vigilance documents and key decision records. The information is not only of value to government but also to the stakeholders outside the government who may misuse the information to their benefit. The increase in outsourcing activities where data is with the third party increases the risk of data loss.

DLP Solution

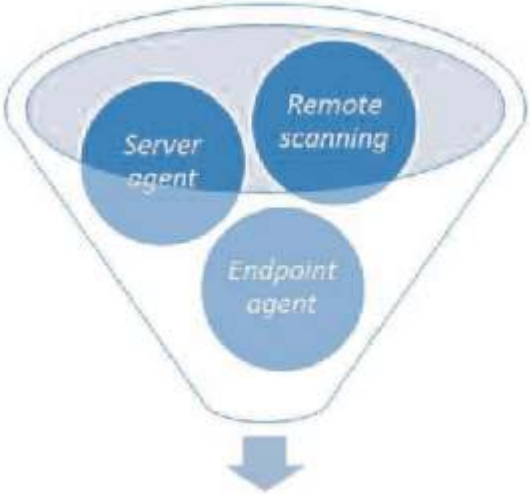
DLP solution can be defined as set of Products and Solutions, based on central policies, identify, monitor, and protect data. DLP Solution can be classified as below.

- **Scope of the Solution:** A typical DLP solution should address centralised management, policy creation, and enforcement workflow, dedicated to the monitoring and protection of content and data. The user interface and functionality are dedicated to solving the e-governance issues and technical problems. It also has to include features like detection and enforcement capabilities.

- **Policy Enforcement:** Policy definition and bringing it in as office orders/guidelines is the core part of the DLP solution. Enforcement of the policy is the key. Strict policy implementation and plugging the gaps on continuous basis and policy revisions based on the incidences reported is essential. The first and foremost is that the departments must define clearly, what constitutes sensitive information and identify the data to be protected on priority and set the policy clearly. The policy should be defined unambiguously and enforced. Besides such clear-cut policies, organisations must deploy DLP solution which covers all stakeholders inside and outside the department who have access to the data. Any device including the laptop should be covered in the DLP solution to prevent data leak. Sensitive data getting into wrong hands can be prevented through encryption.
- **Continuous monitoring:** Monitoring is a continuous exercise and sufficient resource requirements for monitoring need to be planned accordingly for an effective DLP implementation. Content discovery tools for deep content continuous analysis are needed. Some of the content analysis techniques include partial document matching, database fingerprinting (or exact data matching), rules-based, conceptual, statistical, predefined categories, and combinations of the above. They offer far deeper analysis than just simple keyword and regular expression matching. Ideally, DLP content discovery should also offer preventative controls, not just policy alerts after violations occur.

Deploying a DLP Solution

Before deploying a DLP solution one needs to be sure that all other basic security solutions are in place to make the DLP solution more effective. DLP products inspect the content as it moves across the network (real-time) and enforces policies so that confidential information is protected. DLP technology is a suite of products configured at various levels and requirements. Departments need solutions that provide real-time detection, analyze behaviour against the established policies and practices, address all audit requirements at all levels, monitor effective control of critical data and enhance coordination amongst various stakeholders in the system. DLP solution has to deploy the content analysis techniques to find policy violations. Different techniques are deployed such as remote scanning, server agents, network endpoint violation checks based on the policy, need and monitoring needed. A good content discovery tool will understand file context, not just content. For example, some tools can analyze access controls on files and use the corporate directory to understand which users and groups have what access.



Analysis of data at rest

Data at rest is managed through

- Remote scanning for shares, encryption and violations. But care need to be taken not to degrade the network performance. Bandwidth throttling may be necessary to limit the network impact.
- Light weight server agent to scan each server. The agent scans the server locally and can be tuned to limit the performance impact and results sent securely to the central DLP solution management server.
- Endpoint agents with discovery capabilities, USB blocking/monitoring, network bandwidth, unusual leakage etc.
- Re-usable DLP components integrated in application to understand local context and possibly enforce actions within the application system.

DLP is neither an out-box-solution nor a onetime solution. It has to be constantly monitored and improved with new policies and measures to curb the data leak. DLP is a very effective tool for preventing accidental disclosures and planning better policy and processes around the sensitive data.

Edited by: **R Gayatri**