



E-Merging DLP (Data Leakage Prevention)



Author:

Moez Hemani, IT Security Specialist in Emirates Group IT.



Abstract

Data Leakage Prevention (sometimes termed as Data Loss Prevention or Extrusion Prevention) is one of the most hyped and least understood tools in the security arsenal today. Thus to offer an insight into the practical application of DLP within organizations, this White Paper aims at focusing on the areas of control that today's DLP solutions offer along with the ideal methods of evaluating and implementing DLP. The paper also focuses on offerings that latest DLP solutions present which can be utilized to nullify the need for various other 'point' solutions required to secure your infrastructure. Along the way it also highlights some key elements to consider when 'Thinking DLP'!



Understanding Data Leakage Prevention

With business and organizational dependency on IT increasing daily, data today sits at the heart of the information assets priority list. Businesses around the world are growingly concerned about preventing data loss. High profile cases have involved major retailers, credit card industry companies and government agencies having suffered well-publicized data breaches. All enterprises today therefore face a risk to the possibility of unauthorized 'extrusion' i.e. outflow of sensitive information (intentional or accidental) by internally or externally oriented threats. One of the most important security functions today therefore is protection of organizational information assets such as intellectual property, strategic and classified information, personal data of employees, and customers – in (security) terms classified as 'Data Leakage Prevention' (DLP).



As far as the understanding of DLP is concerned, some organizations consider encryption or USB port control as DLP while others limit themselves to implementing industry renowned product suites for different avenues of data loss. Due to the variety of sensitive information resources that reside within today's organizations and numerous means of data leakage possible, it is imperative on their part to implement a holistic Data Leakage Prevention program so as to prevent loss of confidential information, either deliberately or accidentally through all mediums of extrusion possible.

Remember:

- Data loss is more of an internal threat than something that originates externally. It is also more often accidental (lack of employee awareness and negligence) than intentional.
- On account of the losses, legal implications, liabilities and damage to reputation associated with leakage of sensitive information, protection against data loss still sits at the top of most CIO's priority list for a third year in a row¹
- In order to have an effective DLP strategy, rather than concentrating on individual areas of concern, focusing on protection at all avenues of data loss is necessary.

The following section will discuss the different areas of control offered by DLP solutions along with the ideal methods for determining which DLP solutions would suit your environment.

¹ Source: Forrester Research



What DLP Solutions have to offer

DLP by definition is a combination of processes and systems that identify, monitor, and protect Data in Use - DIU (e.g. at endpoints on workstations and laptops), Data in Motion – DIM (e.g. on the network through the use of Internet, email, instant messaging, FTP etc), and Data at Rest – DAR (e.g. within data stores, SharePoint sites, Documentum servers etc) through deep content inspection and with a centralized management framework. It is therefore imperative to understand that protection of data from traversing out of the bounds of an enterprise needs to be managed through all the above avenues of extrusion and today's DLP solutions offer the capability to closely achieve that.

Though several reports on this subject might term today's DLP solutions as being in their 'semi-adolescent' stage, they've matured enough to cater to most requirements and avenues of data leakage up to a considerable amount of granularity, not to mention that there's definitely scope for improvement and tomorrow's DLP solutions will be capable of being called 'mature' in their truest sense. Through deep content analysis and all round protection, today's DLP suites are capable of achieving control over data loss to a significant extent. Below are few examples of the capabilities of new world DLP solutions followed by some instances in the form of simple statements to facilitate in recognizing what level of control over data loss can be achieved.

DLP Capabilities:

'Content' & 'Context' based Data Classification: DLP suites allow organizations to classify data based on Data patterns (credit card number patterns, patterns of financial information, specific blueprints of IP or based on several predefined modules), Data location (on your critical intranet sites, outputs of certain applications, on network drives etc) or particular forms of Data (e.g. all AutoCAD design documents).

Policy enforcement: A wide range of restrictions on the ways that data can be transported out of the organization may be applied in the form of blocking data transfer, encrypting data; prompting users for a justification of their action or just passively logging the action. Restrictions on copy, paste, print screen, network copy/paste, file upload/sharing (HTTP, FTP, IM), content (text) upload on internet, transfer to all forms of removable media (USB, Bluetooth, Disc Drives, smart phones etc) and printing restrictions can be easily achieved.

Reporting – Passive analysis and reporting on user behavior around violations, most common avenues of data loss, top list of employees/departments committing violations, top form of information against which violations occur etc can be accomplished to give a very good understanding on how controls can be applied or improved.

Awareness – A good byproduct of DLP implementation within an organization is along the lines of employee Awareness. Features of new world DLP suites such as prompting users with warning / information messages referring to corporate policies when committing a violation or requesting justification via a pop-up window on their data transfer actions also serves to bring about awareness within the workforce. This also serves to hinder future acts of attempts to transfer sensitive data out of the organization and can bring about a gradual cultural change in the way employees see organizational data.

Add-ons – In addition to offering what they do, DLP solutions are also built with the ability cater to other security needs for which organizations would normally choose to implement 'point' solutions. Making use of such add on modules that DLP suites offer can assist enterprises in achieving centralization, standardisation, integration and many-a-time cost control. Examples of such areas are Email encryption; file and folder encryption / hard disk encryption, removable media encryption, protection of data at handheld devices and user awareness features / user behavioral analysis - to a certain extent.

Remember:

- DLP solutions today are deeply content aware - therefore realizing control within your environment that relates to an example statement such as "We need to block / encrypt any document containing credit card numbers (or any other pattern for the matter that could classify the document as confidential) being sent out of bounds of the enterprise network though Email/IM/FTP/USB by an employee of grade less than a 'Manager' if he / she is not on the office LAN" – IS POSSIBLE.



- DLP solutions can offer additional functionalities that are offered by other 'point' security solutions. One may therefore choose to implement these to achieve standardisation and integration (not to mention cost control), therefore making best use of what DLP has to offer.

The next section describes the ideal approach which can be selected in order to evaluate and implement a DLP solution within your environment.

Evaluating and Implementing DLP

Evaluation of DLP suites to choose the solution that best suits your environment is one of the most critical steps in the entire process of working around DLP. The first step in this approach is to determine specific requirements of your environment from a perspective of data leakage in the form of definitive test cases. This is highly recommended as DLP when put into practice will target the entire user community within your environment and one can't afford to go wrong with that. Evaluation against detailed test cases will ensure that the product delivers exactly to your requirements. Also, since DLP offerings range from simple removable media control to complex controls such as determining sensitive information residing on your SAN / NAS environment, attaching policies to them and applying controls - creating definitive test cases are crucial in analyzing product capabilities so that they can be best put to use.

A statistical scoring mechanism may also be used to shortlist DLP vendors that, at a high level, satisfy requirements documented in these test cases. A thorough technical proof of concept in a laboratory environment with the top vendors of choice (which for most organizations would be market leaders within the DLP space²) would add great value as practical tests would ascertain the product's capabilities of realizing requirements that were simply noted down as the 'goals' for your organization.

As mentioned earlier, since the implementation of DLP within an organization targets the operation of its largest community – i.e. The Employees, a well thought through strategy on implementing DLP within an organization should always involve first defining what data is confidential, its form, content, context and location. Later, employing DLP in a 'passive-only' mode for its initial part and observing user behaviour / violations without actually 'blocking' – this can be termed as 'Trend Analysis' - would immensely help an organization and act as a feed for defining DLP policies to actually prevent data breaches. Such an approach would ensure that implementation of restrictive policies cause the least operational hindrances which may adversely affect business operations.

Remember:

- Create detailed test cases for evaluating DLP products based on the requirements of your organization. Rate each test case based on priority and attempt to apply a scoring mechanism to assign the final scores to each DLP suite. This makes the result more tangible and presentable to executive management.
- In order to help you build test cases, apply thinking in the direction of the three avenues of DLP i.e. Data in Use, Data at Rest and Data in Motion and apply how sensitive data in your organization can leave its bounds through these avenues.
- Implementing DLP within an enterprise is a challenging task as it in a way 'meddles' with normal user behaviour. Employing the 'Trend Analysis' technique before actually forming restrictive DLP policies can save huge operational hassles.

Conclusion

DLP is an enterprise wide initiative in all senses – from each possible avenue of data loss (virtually through all means of escape) to the segment of an Enterprise it targets (the Users). In order to achieve the most success from it in your environment, a holistic DLP program is essential. The product that an enterprise chooses for achieving its DLP goals will determine the effectiveness with which its objectives are met. Therefore a sophisticated evaluation procedure to determine what best suits your needs would add great value in working towards these objectives. Once this is ascertained, implementing DLP can be made a lot easier by following a 'Trend Analysis' based

² Recommended reading - Gartner and Forrester research reports on DLP for 2010



approach to establish a good hold on user behaviour and perceive the cores areas of data breaches. Pursuing this step-wise methodical approach should ensure a smooth DLP roll out, not to mention the Brownie Points for us Security Managers