



5 Essential Ingredients to a Data Loss Prevention System

1. Comprehensive channels coverage.

It is impossible to predict which outbound channel the next data leak will occur. Some expected avenues are: corporate email, private email, webmail, blog, instant messenger, P2P application, internal web or FTP server etc. Therefore, the DLP system must cover ALL the relevant channels. The majority of "DLP" systems do not even try to cover all network channels. Typically, they cover SMTP, FTP, HTTP (client side), sometimes HTTPS and instant messaging.

This coverage is further handicapped. For example, scanning SMTP, these systems require integration with the corporate email server and inspect only emails sent through it. Emails sent through an external ISP are overlooked. Emails accessed from outside the perimeter through POP3 or HTTP (server side) are ignored by such solutions. The dangers of file sharing applications and exposure of the internal web servers are disregarded.

2. Enforcement

Data Leak Prevention, by its definition, requires electronic enforcement of the data security policy – i.e. the product must be able to effectively block transmission of protected data.

Many "DLP" products being sold are actually DLD – Data Leak Detection products. They are designed to report what data breaches have occurred, instead of stopping them in real time.

3. Content Inspection

The true DLP solution must inspect content. Making decisions based on the form (file type, file attributes etc.) or meta-data (author, language, size of attachment etc.) is not enough.

4. Accuracy

The DLP solution must be sufficiently accurate. Among two types of errors (false positives and undetected leaks) the more dangerous error is a false positive. In the enforcement mode, even a small amount (0.1%-0.2%) of false positives can wreak havoc in the organization. **Therefore, a DLP solution has to employ detection technology with virtually zero false positives.**

Another aspect of accuracy is that the DLP system must protect data and not a specific form of its representation. Therefore, the DLP system must be resilient to typical modifications of the data, such as excerpting, embedding, changing file format, re-ordering, re-typing, text re-formatting etc.

5. Non-duplicating protected data.

The DLP solution must not duplicate the protected data in any form! If it does, then DLP becomes Data Leak Provoking. But many vendors still sell products, copying the data they are supposed to protect into their internal database.

Encrypting such data, or keeping it in the form of the search index is not enough to satisfy this requirement!

GTB Technologies, Inc.

5000 Birch St. Suite 3000 • Newport Beach, CA 92660

800.507.9926

www.gtbtechnologies.com