

DLP and IRM...

# What Can the Combination Do?

In securing unstructured data, there's a lot of confusion over which technology is best in what context. DLP and IRM solutions can combine to give organizations the most on of their investments in terms of better, more effective security at a lower cost.

Over the past few years there has been a lot of marketing expenditure on various solutions for protecting unstructured information (e.g. emails, documents, designs, drawings) of the enterprise. Solutions range from basic 'port blocking' technologies which rely on controlling USB, CDs etc. to high-end Data Loss Prevention (DLP) and Information Rights Management (IRM) technologies.

Therefore in the layman's terms there is a lot of confusion on which technology fits with what business context and need.

Before we come to the solution, let's look at the problem of securing unstructured information a little carefully. Unstructured

information goes through a life cycle of create - store - transmit / collaborate - use - archive - delete. The information security needs of an enterprise will typically be defined by what stage an enterprise wants to acknowledge the presence and then secure information.

A completely 'aware' enterprise will have mechanisms to discover information, monitor its flow, protect it to ensure compliance with information security and access policies and also maintain an audit trail for the various activities performed on information and its copies.

**What does a DLP do:** A content-aware DLP system discovers data lying at various

locations like desktops, file servers and databases. It classifies them into various 'filing cabinets' based on centrally defined content patterns. It monitors and controls the flow of this information based on centrally defined policies. Let's consider a case of a person having credit card details on his computer in a document. A DLP system will:

- 1 'Discover'** the presence of this document on the user's computer and 'classify' the document into the 'Credit card data' cabinet
- 2 'Protect'** the flow of this document, for example it should not be emailed outside of the organization, Cannot be uploaded on any website
- 3 'Audit'** the flow of this document, for instance 'The document was sent to a colleague,' the document was 'attempted to be copied to a USB storage device'

**What does it not do:** DLP policies are applicable to information within the enterprise. Once information moves out to business partners then the DLP policies are no longer applicable. The DLP system does not encrypt information, so in cases of device theft, data can be compromised.

**What context is DLP useful in:** A DLP system is useful in contexts where data is lying in heterogeneous systems and enterprises need to start with a method of 'discovering' their own data. This 'discovery' typically leads to formulation of rules and policies for protection and audit compliance to regulatory frameworks such as ISO, SOX and GLBA.

**What does an IRM do:** An IRM system encrypts the information and associates a 'usage policy' with each piece of information. The usage policy typically governs WHO (users / groups, within / outside of the enterprise) can use the information, WHAT (read, edit, forward, print) can each person do, WHEN (after a certain date, for a defined time period) can this be done and from WHERE (from official laptop only). The encryption and the policy is associated through out the lifecycle of the information. An IRM system will:

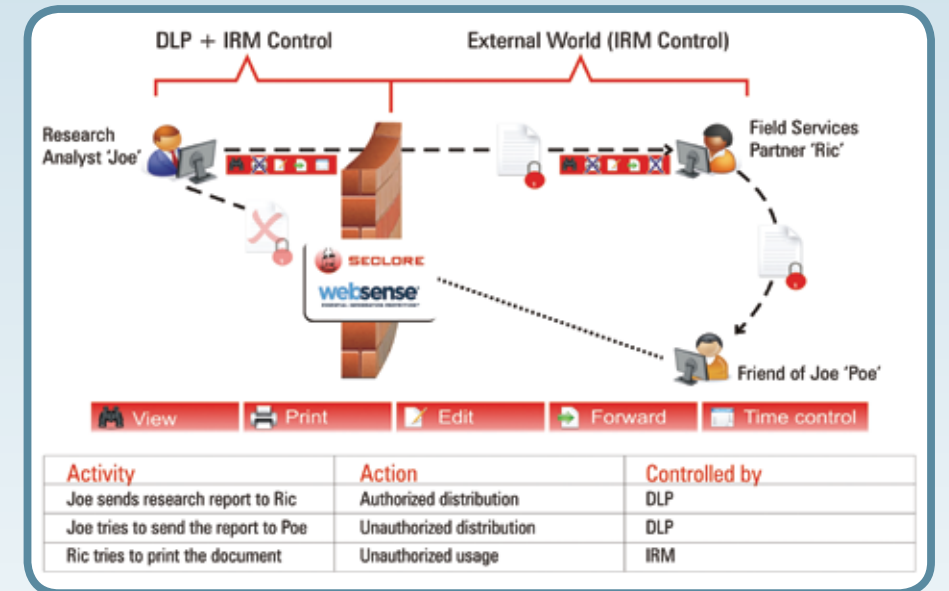
- 1 Define** a usage policy whereby a power user can define the WHO / WHAT / WHEN / WHERE for different kinds of information for example Board communication can only be accessed by internal and external board members and the company secretary.
- 2 Implement** policy controls by ensuring that usage of information is as per the defined policies, for example forward looking financial statements should not be circulated before Tuesday morning.
- 3 Audit** the usage of information by centrally reporting WHO has done WHAT with the information, WHEN and WHERE.

**What does it not do:** An IRM system does not put controls on the movement of information like blocking e-mails and Web uploads. Controls are implemented when information is being used. An IRM system also does not typically discover or classify the data and therefore is dependent on 'events' to protect data. The events could be 'on creation,' 'on attachment to e-mail,' 'on upload to sharepoint' and so on.

**What context is IRM useful in:** An IRM system is useful when information usage policies need to be implemented in a highly collaborative environment which includes internal and external stakeholders. It is also useful in cases where information control and monitoring needs to be granular to be in compliance with regulatory frameworks.

**Why would you need both the solutions?**

A combination of IRM and DLP systems like those provided by Seclore (Seclore FileSecure) and Websense (Websense DLP) helps



in the discovery, protection and auditing of information usage and flow. In this case the combined Seclore and Websense solution streamlines information classification, protection and auditing by automating policy-based controls. The content-aware Websense Data Security Suite eliminates the need to manually classify and secure

files, while Seclore FileSecure then automates and extends the appropriate security controls to the files and emails. The integration helps organizations maximize their investments in IRM and DLP for better, more effective security at a lower total cost of ownership.

**A combined DLP and IRM solution enables business workflows while protecting sensitive information. Benefits include:**

- Extending DLP policies outside the enterprise perimeter
- Lowering IT administrative overhead through automated application of content-aware policy controls
- Facilitating compliance and auditing of 'unstructured' data (e.g., PDFs, MS Office formats, email, Web pages) inside and outside the organization
- Enabling collaboration involving new technologies, such as dynamic Web-based applications
- Maintaining business workflows while securing sensitive data ■

**For comprehensive data protection strategy, organizations can now choose DLP and IRM in a complementary combination."**

.....

VISHAL SALVI  
Senior VP and CISO, HDFC Bank

*This feature is brought to you by IDG Custom Solutions Group in association with*

**Seclore & Websense**

