AUTOMATING DATA CLASSIFICATION AND ENSURING SECURITY AT DEPARTMENT LEVELS

One of the key reasons for the failure of existing security systems, such as DLP, is the lack of on-going data classification. New information is being created on a regular basis in a decentralized manner in different departments and has to be classified as soon as it is produced. Unfortunately the process of data classification is a tedious and time consuming one requiring the information owners/department heads to manually analyse huge amounts of information, gather details of what they think is sensitive, and send it to central admin for monitoring purposes. Considering the fact that information owners are busy individuals this process starts to hit delays resulting in security gaps.

1 THE SOLUTION: E-SAFE COMPLIANCE ENSURES SECURITY IS EVERYONE'S RESPONSIBILITY

e-Safe Compliance gives special attention to data classification. The fundamental difference between e-Safe Compliance and DLP systems is that it treats data leakage as a business problem that needs to be tackled at an **operational level, rather than an IT problem**.

1.1 SECURES INFORMATION AT ITS SOURCE, AS IT GETS CREATED, ENSURING THAT INFORMATION IS PROTECTED ALL THE TIME.

e-Safe Systems recognized the fact that users are generally busy and can't spend much time securing information. e-Safe Compliance solved this problem by securing information at its source, encrypting sensitive documents using **persistent universal encryption.** Documents encrypted using universal encryption can only be opened on devices having the e-Safe agent installed, along with the relevant user credentials, and are tracked throughout their lifecycle from creation to deletion using e-Safe. As such, if the users decide to send the documents to a 3rd party, or decide to copy them, they need the e-Safe agent to open them.

1.2 MONINTORING REAL SENSITIVE INFORMATION USING DECENTRALISED AND CENTRALIZED DLP RULE CREATION

e-Safe compliance offers both centralized rule creation as well decentralized rule creation. Information owners using the **information tagging utility** can categorize large amounts of information themselves, without involving the central administrators, and create DLP rules. Further the information owners also receive reports on the usage of sensitive information which they have defined. This encourages them to carry out this function as they are able to see how their information is being used.

Apart from decentralized rule creation e-Safe Compliance offers centralized rule creation which allows admin to define generic organization wide monitoring rules.

1.3 PROTECTING HIGHLY SENSITIVE INFORMATION USING DOCUMENT RIGHTS MANAGEMENT

e-Safe Compliance solves the problem of classifying highly sensitive information by providing a built-in **document rights management module** which allows top management to define sensitive documents. Users can simply right click on a particular document and define the following:

1. Define the classification for the sensitive documents as being
    a. Secret
    b. Confidential
    c. Office document
2. Define who can have access to the said information
3. Define the usage restriction on the information such as cut/copy/paste/print etc.

More importantly information owners receive usage reports on the use of their particular information. This ensures that, if there is any misuse, the information owner who understands the importance of that potential misuse is in a position to take appropriate action.

1.4 CLASSIFYING INFORMATION IN FILE SERVERS, SHAREPOINT AND DATABASES.

In most organizations most of the information resides in Datastores. e-Safe Compliance, using its **Server side scanner** technology can scan existing and new information being created in file servers, databases and Sharepoint. Information detected is classified according to the relevant rules and its' usage is tracked.