LITERA MICROSYSTEMS
REPUTATION MATTERS

Litera Microsystems on...
Data Loss Prevention

Data Loss Prevention (DLP) is an organizational imperative to avoid potential security breaches by preventing the loss or misuse of sensitive data. This mission is backed by an entire industry of DLP software and services that are configured and trained to understand what is considered sensitive information, then monitor it and prevent it from getting into the wrong hands.

Maintaining the integrity of information security within law is a top priority. Firms take every precaution necessary to prevent confidential and/or proprietary information from accidentally being distributed. To protect the reputation of the lawyer and the firm, DLP measures are in place to block certain information from being sent, shared, or downloaded.

THE CHALLENGE: SECURITY WITH A SENSE OF INTELLIGENCE

Reducing risk is mission critical, but so is communicating efficiently and effectively with clients. The nature of lawyer and client communications requires frequent exchange of sensitive information and traditional DLP solutions have proven, in certain scenarios, to be too disruptive to the lawyer's workflow.

Finding the middle ground between an unprotected email transaction and DLP is a challenge—how can the Information Technology (IT) team protect sensitive information from ending up in the wrong hands while delivering solutions that fit the lawyer-client culture with a sophisticated level of intelligence around information sharing?

YOUR SOLUTION: LITERA MICROSYSTEMS

At Litera Microsystems, we believe the solution is in a combination of sensitive data management tools that have DLP-like features; features that help control and monitor the exchange of sensitive information without major workflow disruption. Our view of sensitive data management within the legal sector is one involving three layers of security: recipient control, clean documentation, and active monitoring.

The Litera Microsystems 3-layer DLP model

Layer 1: Clean Documentation

DLP protects against sensitive data from being distributed, including attaching documents with hidden metadata. Litera Microsystems makes it easy to clean risky data from emails and attachments with its Metadact® solution. Metadact provides comprehensive metadata management to protect against financial risk, data leakage, possible malpractice due to inadvertent disclosure and, above all, loss of reputation. Regardless of the device or email method, Metadact ensures thorough metadata scrubbing of every file to reduce risk and ensure your data remains secure.

Layer 2: Recipient Control

A key component of DLP is the ability to restrict users, user groups, and domains from gaining access to sensitive information. Hundreds of organizations across the world turn to Metadact not only for its cleaning capabilities, but for its recipient control functionality, too. Metadact prevents users from making common email mistakes, including improper formatting, inaccuracies using Reply All, BCC, or the Multi-thread feature, and auto-completion inserting unintended email addresses.

Layer 3: Active Monitoring

IT leaders face the complex responsibility to monitor the movement of files and attachments across—and outside—their network. At Litera Microsystems, we continue to explore ways in which our solutions can be part of an overarching DLP rule set. Our customers have provided us with excellent insight into approaches that avoid workflow disruption, and we continue to investigate this as a priority area.

With Litera Microsystems, lawyers can work independently and autonomously with confidence. Contact us to learn more.

Litera Microsystems is the leading provider of software for drafting, proofreading, comparing, repairing, and cleaning documents in the legal and life sciences industries worldwide. Our core products empower users to generate, review, and distribute high-quality content quickly and securely, from any device. Today, Litera Microsystems supports thousands of document-intensive organizations across the globe, helping them satisfy the complex demands of clients and regulators.

Reducing risk is mission critical, but so is communicating efficiently and effectively with clients.