DLP: Protecting You From Yourself

BY BRIAN PODOLSKY

There's an arms race in legal technology. Fueled by increasingly complex security audits and consumer technology, clients and attorneys alike are making more demands of their law firms, which are, in turn, making demands of their document management system (DMS) vendors.

To meet these demands, new entrants into the DMS market are specializing in data security and augmenting the established content management systems. A "need-to-know" security model, in which only those specifically assigned to a particular matter have access to its contents, has sprung into the lexicon of many CIOs and CISOs.

But what if "need-to-know" isn't enough? How do you protect data even from those attorneys and staff who legitimately have access to the content? This is where Data Loss Prevention (DLP) comes in.

Going Beyond Need-to-Know with DLP

You can think of DLP as a solution that is designed to save the users from themselves.

DLP ensures that actions performed on work product meet both client and jurisdictional rules and requirements. For instance, an attorney may have full administrative permissions to all matter content, but may not realize that specific content is not allowed to be emailed to a European domain. DLP would prevent that action.

Actions that lead to data loss are, in the vast majority of cases, not performed maliciously. Rules enforced by DLP are meant to protect data from the naïve or hurried user.

Corporate America is already familiar with DLP. Vendors such as Symantec and Digital Guardian have been offering DLP solutions to large enterprises for years. But DLP is fairly new to legal technology, since many of those enterprise DLP solutions failed to integrate into legal platforms, where client and matter assignments reign supreme. Major legal DMS vendors are now entering this paradigm.

iManage Extends Security Policy Manager and Enhances Threat Manager

iManage has made incredible strides in the security realm over the past two years. Security Policy Manager (SPM), part of the iManage Govern Suite, provides firm with a straightforward approach to achieve the "need-to-know" security model. With upcoming integration with RAVN technology available in iManage Insight, knowledge managers can rest assured that content and expertise are managed properly even in a secure environment.

In the area of DLP, iManage also recently announced integration between SPM and the Workshare Secure product. The integration allows privileged client and matter content to be emailed only to a list of sanctioned internal and external email addresses associated with a policy on a matter. Configurations give firms the choice to block email to non-sanctioned parties altogether or allow the email to be sent while simultaneously raising an alert and report on the policy violation. The "allow-but-report" model lets the attorney continue working, but also informs the risk team of what is happening with the data.

iManage Threat Manager, a key part of the Govern suite plays an important role in protecting sensitive data and preventing data loss by detecting modern day security attacks and intervening in near real time. Typical threat patterns iManage Threat Manager surfaces include the abuse of privileged accounts, departing laterals taking non-sanctioned client material, insiders accessing matters they have not billed to and more. In upcoming releases, iManage has announced intelligent frameworks to facilitate intervention including the ability to disable an account for well-defined threat patterns.

iManage's RAVN technology holds a lot of potential. As an observer, I would be excited to see future considerations include leveraging RAVN technologies to integrate with the iManage Govern Suite to prevent actions based on RAVN identifying sensitive information as well as prioritize alerts based on the classification of the underlying content.

NetDocuments Introduces a Native DLP Solution with AI

NetDocuments, the other leading legal content platform vendor, has recently announced plans for its own DLP solution. Unlike iManage, NetDocuments DLP would not require any other third-party products.

Built into the service itself, NetDocuments's DLP solution leverages AI and data extraction to identify content with sensitive information. Rules would be created to prevent documents with personally identifiable information (PII) or personal health information (PHI) from being emailed externally. In addition to these dynamic or smart rules, more general client- or matter-specific rules can be created to prevent certain actions (email, download, print, etc). The end vision is to also provide geo-fencing, which designates geographical areas to and from which certain documents can be sent or accessed.

So far, I have covered how to prevent data from erroneously leaving the confirms of the firm's network. But the term "Data Loss Prevention" does not simply refer to data leaking out of the organization. Data loss prevention also includes keeping data intact.

Syncing to the Cloud

With the proliferation of consumer-friendly collaboration services such as Dropbox or Google Drive, many attorneys have embraced the idea of having local folders synchronized to cloud repositories. The ability to always have the latest copy of your files from any device is an enticing feature. NetDocuments provides this feature-set with its ndSync product. iManage will be releasing its iManage Drive product in the near future. Both of these applications are designed to allow recently edited content and entire matter workspaces to be replicated and synched to a local drive. With two-way synchronization, attorneys can now easily work on content while on the road. Then, when they connect back to the network, all local changes are uploaded to the DMS, and all DMS content updated by teammates are then synched down to the local drive. Naturally, this capability leads to the fear of large-scale destruction of data due to malware or crypto-locker viruses. Thankfully, ndSync includes ransomware protection kill-switches. If the application detects Ransomware encrypting multiple files, the synchronization to the cloud is automatically broken, protecting the production repository. When released, iManage Drive will include this functionality as well.

Balance Security with Ease

The trick is increasing security without putting too much of a burden on the attorney's day-to-day operations. How can you confidently protect the firm's data while making it as easy as possible for the partner working on the case? Some organizations may decide to implement the "allow but report" method of DLP (although perhaps not for the most sensitive rules). If a Digital Rights Management solution like Azure Information Protection (AIP) is then used to encrypt the content on its way out, then the firm would have even greater control of the content. If there is a report of a secured document being emailed externally, the security manager can revoke access at any time.

Hackers and malicious actors know that the crown jewel of a law firm is its document repository. High profile security breaches have splashed been splashed in the headlines, but there are many more security breaches that never made the papers. Increased security audits and regulations from the healthcare and financial sectors have forced firms to tighten the lasso around their content. Much has changed in the past few years. To be successful, any legal DMS provider must not only meet the demands of its current customers, but also anticipate the future demands of the entire market. **ILTA**

Brian Podolsky leads the Enterprise Content Management (ECM) Practice Group at Kraft Kennedy. He has extensive experience implementing and supporting Microsoft Office, NetDocuments, iManage, OpenText eDOCS, and Worldox document management systems, as well as third-party integrated add-ons. He also drives research on the latest ECM technologies including email management, enterprise collaboration and search, and provides guidance and best practice standards to clients implementing ECM solutions.