PROTECTING YOUR DATA WITH DRM AND DLP

BY BRIAN PODOLSKY

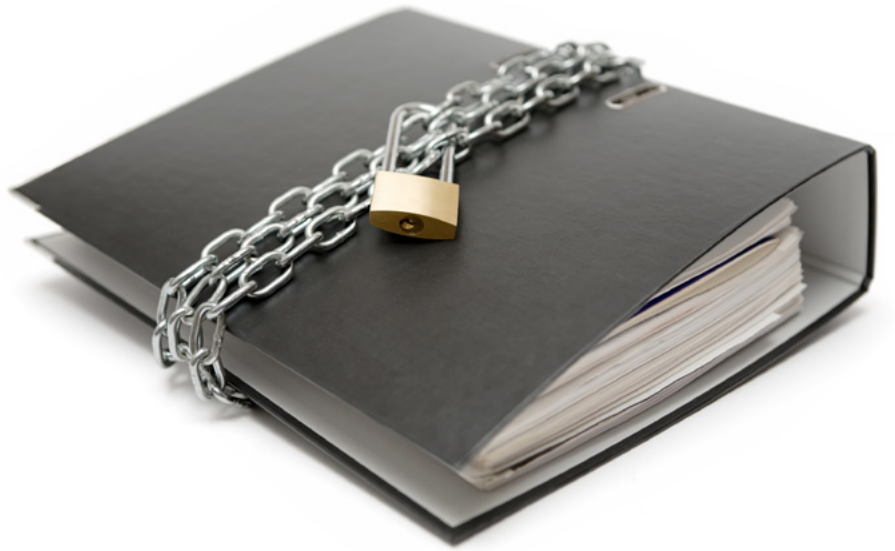
With a streamlined DRM solution and integrated DLP, businesses can be sure they are doing everything possible to protect their most sensitive information.

Blockchain and AI might be happening buzzwords in the industry, but when it comes to security, there are two other technologies that have been making an impact over the past several years: digital rights management (DRM) and data loss prevention (DLP). You have probably had some experience with DRM in your everyday life, even though you may not have realized it.

Ever wonder why you couldn't simply share a song you bought on iTunes with a friend? That's DRM. The song itself is digitally signed and secured to your

Apple ID, and can only be shared from 'authorized' computers. Long gone are the days of freely downloading MP3 files that could be copied from listener to listener. The music industry needed control over its product, so it made sure content could be tied to the purchaser or specific devices/accounts using streaming services.

Another famous (or infamous) foray into DRM was made by Keurig, maker of coffee machines and single-cup coffee pods. Keurig wanted to ensure that customers could use only its proprietary K-Cup coffee pods in Keurig machines. The machine would read a special ink to ensure that the pod was Keurig-approved before allowing the coffee to brew. In a classic case of DRM gone wrong, customers reacted with anger and Keurig's share price fell. The company apologized to its customers in 2015 and issued an adaptor to disable the DRM functionality.



Rights management

DRM has to be used properly. The challenge has always been to apply digital rights as seamlessly as possible to avoid the frustration that Keurig customers felt. How do you apply DRM so that it is not a headache for your employees?

In the corporate world, vendors such as Seclore have focused on applying DRM to company work products. Such solutions put a security wrapper around a document, providing information on who, what, when, where and how that file can be accessed. To apply DRM security, Seclore uses policy federation, translating the security of a content system and applying that security to the content protected by DRM.

Let's take a look at the example of a SharePoint document that is secured within SharePoint to your finance director. If that file were to be downloaded and stored outside SharePoint, Seclore would seamlessly add the finance director's email address as a valid user with access to that file. No one else would be able to access it. In addition, when sending a DRM file through email, Seclore can automatically add the email recipient to the access control list on its way out the door.

The next challenge is how to make it easy for recipients to view content that's been protected by DRM. This is where a lot of DRM vendors falter. Many require some sort of agent or software installed on the recipient's machine. Some offer a light agent that can be installed into the user's context without administrative privileges. However, many firms restrict what programs users can install, so these agents require assistance from a firm's IT support team. Yet more solutions allow you to view the secured content in a web interface. None of these are particularly elegant, but vendors do offer a few options to meet the security requirements of most firms.

> *How do you apply DRM so that it is not a headache for your employees?*

Loss prevention

DLP doesn't have as many flashy or public-facing use cases, but security-conscious firms have been implementing it for several years. DLP is used to ensure that sensitive information does not leave the confines of the internal network.

DLP solutions identify content with personally identifiable information (PII) such as birth dates, mothers' maiden names and social security numbers, and ensure that content cannot be placed onto USB sticks or sent via email. We are starting to see DLP enter the space of content management solutions.

NetDocuments recently announced NetDocuments DLP as part of its Governance module. This solution draws

on data classification to identify content with PII and PHI (protected health information). In addition, DLP rules can be set at the matter level to restrict actions such as downloading, copying, attaching, and sending links. Rules can also be created to confirm location, essentially putting a geo-aware wall on where that content can be downloaded. Not only are you protecting the content, but you are protecting the user as well. This is meant to protect the naïve, unaware or distracted employee, in addition to the malicious one. It protects every action by every user, even if the user may have been given full security access to the document.

'It is more than border protection,' says NetDocuments CTO Alvin Tedjamulia. 'It is more than after-the-fact monitoring. DLP is action protection for every user, regardless of the access control list or ethical wall.'

DLP versus DRM

There are a few different ways to look at the differences between DLP and DRM solutions. DLP can be thought of as a more proactive model. With DRM, an employee who is leaving the firm in a week can legitimately access all matter files and export them out of the firm's content system. This behavior can be audited and, if necessary, that user's access can be revoked later through the DRM solution. If the matter is protected by a DLP shield, however, the large export would not be allowed to occur in the first place.

Another difference relates to the functions a user with full access can perform. DRM allows a user to share and control overall access to the document. DLP, on the other hand, prevents actions such as emailing or forwarding when a document happens to have PII or belong to a particular matter—saving users from themselves.

Why choose?

Another option is to combine the power of DLP and DRM. Some DRM engines, for instance, can integrate with DLP solutions to protect documents with sensitive data automatically as they are shared. By itself, DLP does not add security to a file that has been marked as sensitive. It just prevents certain actions. Combining your DLP and rights management streamlines and automates your data security program.

Tedjamulia has referred to DLP as 'the new frontier of security'. With a streamlined DRM solution and integrated DLP, businesses can be sure they are doing everything possible to protect their most sensitive information.

Brian Podolsky leads the Enterprise Content Management (ECM) Practice Group in the New York office of Kraft & Kennedy. He has extensive experience implementing and supporting Microsoft Office, iManage, NetDocuments, OpenText eDOCS and Worldox document management systems, as well as third-party integrated add-ons to these systems. He also drives Kraft & Kennedy's 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.