

DRM in ERM: Protecting Digital Rights Inside & Outside of an Enterprise

IMERGE Consulting, Inc

Robert Smallwood

September 2005

Robert.smallwood@imergeconsult.com

As Appeared in eContent World

www.imergeconsult.com

"If you reveal your secrets to the wind you should not blame the wind for revealing them to the trees."

Kahil Gibran, *Lebanese artist & poet in US (1883 - 1931)*

With the increasing globalization of business, and the sharing of information between companies, their customers and suppliers to far-flung parts of the world, protecting confidential information not only within an enterprise, but also once it leaves, has become paramount.

The gaping hole in security schemes of content management systems is that few, if any, protections exist once the information is legitimately accessed. This confidential information, which may include price lists, patented designs, blueprints, drawings and reports, can often be printed, faxed or e-mailed to unauthorized parties without any security attached. This has given rise to an emerging but critical set of capabilities by a new breed of software companies that develop and sell Digital Rights Management (DRM) software, more commonly termed Enterprise Rights Management (ERM) or Enterprise DRM when organizations deploy it. DRM (alone) is mostly used to refer to protections of digital entertainment files in the business-to-consumer marketplace.

In investment banking, research communications must be monitored, according to NASD regulation 2711, and ERM can help support compliance efforts. In consumer finance, personal financial information collected on paper forms and transmitted by fax (e.g. auto dealers faxing credit applications) or other low security media with can be secured using ERM, even directly from a scanner or copier. Importers and exporters can ensure data security and prevent the loss of cargo from theft or even terrorist activities with it and they also can comply with U.S. customs and fast-changing trade regulations by deploying ERM software. Public sector data security needs are numerous, including intelligence gathering and distribution, espionage, as well as and Homeland Security initiatives. Firms that generate Intellectual Property (IP), such as research and consulting groups, can control and protect access to IP with it, and in the highly collaborative pharmaceutical industry, ERM can secure research and testing data.

ERM software enforces and manages information access policies and use rights of electronic data and documents. Controlled information can be emails, spreadsheets and financial statements, policy and procedure manuals, research, customer and project data, personnel files, medical records, Intranet pages and other sensitive information. ERM provides "persistent" (continual – regardless of where and when access occurs) enforcement of information access policies to allow an organization to control access to information that needs to be secured for privacy, competitive or compliance reasons. But is ERM really so new?

"We've had rights management capabilities since 1994 in Version 2.0 of PDF," states Ryan Hunter, Senior Product Marketing Manager of Security Solutions at **Adobe**. "Even then, you could restrict access to documents, and prevent editing and printing." But this was not a complete solution suitable for use within and outside of an enterprise. For instance, users forget passwords, print rights may need to be revoked after-the-fact, and access rights may need to be revoked so that only the latest version is viewed. This can only be accomplished by enforcing access rules and policies at the server level. "The limitations, though, caused us to develop an enterprise solution," Hunter says. Adobe began shipping, *LiveCycle Policy Server*, in December last year. *LiveCycle* boasts cross-platform support, running on Windows, Linux and MAC O/S servers (in contrast with **Microsoft's Rights Management Server (RMS)**, which runs only with *Windows 2003* servers), which is particularly useful in a multi-

platform collaborative environment, such as manufacturing design or any kind of research conducted by multiple groups.

AirZip, Inc., also has the same cross-platform support, including the aforementioned platforms and also applications running on AIX and Solaris. A distinguishing feature of AirZip's *FileSECURE* is that it can be used for files of any type, not just electronic documents.

Interestingly, one of AirZip's biggest markets is China, since they provide a native Chinese version of *FileSECURE*. But wait, don't the Chinese allow for copying of software and other intellectual property (IP)? Well, yes - mostly. Read on.

Sure, multinational firms basing manufacturing operations in China would be motivated to deploy ERM software to protect IP. But that's not why the Chinese have started protecting theirs.

"It seems that Chinese entrepreneurs have caught the capitalist bug and have been walking off with their (manufacturing) employers' IP documents - and starting up their own firms down the road," says AirZip CEO Gary Clueit. And since protecting IP is tenuous at best in China, there isn't much to stop them. So Chinese firms have started adopting ERM software to protect their IP from employee theft - and potential competition.

"But our rights management implementations in China have to be a little different, since software encryption (scrambling and encoding data, with a software key to provide access) is illegal there. So a hardware device has to be used, which is typically a USB hardware key that is inserted into the PC to unlock access to the information," Clueit adds.

AirZip sets up a hierarchy of roles and access rights in *FileSECURE*: *Superusers* are generally system administrators that set up and define *Organizations*; then managers within *Organizations* set up high-level policies, create users, define security categories and work groups. Then, within *Organizations*, *Authors* create and secure documents and files. When sending documents to those not defined within the hierarchy, "*Dynamic Readers*" can be set up with read-only access to documents, on-the-fly. Documents can be scanned into the system from most high-end Multi-Function Printers (MFP) and rights can be assigned automatically by dragging and dropping documents into predefined folders. What doesn't *FileSECURE* do? It secures entire documents, not just certain areas of them, and although secure annotations can be added, it doesn't do, "secure editing," as some other firms in the ERM space, such as **Authentica**.

"We've been in the ERM space for about seven years now, and we believe we're the marketshare leader," states Mark Overington, VP of Marketing at Authentica. Authentica has approximately 200 customers, but it is difficult to ascertain what percentage of those use its secure email product, *Secure Mail*, and those that use its ERM product, *Active Rights Management* (ARM). Authentica actually delivers the U.S. Presidential Daily Briefing (PDB), giving access to certain pages of the document to those with security access.

Positioned for use in business-to-business and business-to-consumer applications, *ARM* is the foundation of Authentica's full suite of security solutions, including *Secure Mail*, *Secure Documents (for Microsoft Office)*, and *Secure Documents (for Adobe PDF)*. The latest release delivers:

- **Support for all content filtering engines:** Direct support for all e-mail content filtering engines, allowing organizations to send secure e-mails in compliance with regulatory requirements without requiring changes to existing mail infrastructure;
- **Secure point-to-point communications between partners:** Secure delivery of e-mails and documents using a web link notification;
- **Enhanced user control and audit functionality:** Provides direct user control over e-mail access, expiration dates, message recalls and permissions.

Authentica supports *Lotus Notes* email and collaboration, and also EMC/Documentum's *eRoom* collaboration suite. *ARM* runs on Windows 2000 and 2003 platforms.

GigaTrust from GigaMedia Access Corp., Herndon, VA, started up in the year 2000. GigaTrust is in the Microsoft camp, partnering to extend the reach of Microsoft's RMS technology by providing a trusted community for third party authentication based on a secure, public Active Directory implementation.

GigaTrust and its hosting partner, **Data Return**, provide a secure and reliable environment required for mission critical data through a hosted, Application Service Provider (ASP) model.

The latest release of the *GigaTrust Client Software* provides the ability to protect WordPerfect files, DICOM (radiological images) files, media files, Corel files, Visio files, and other vertical industry content. It already could manage rights for Quattro and PDF files as well. The GigaTrust software works by wrapping sensitive content in a RMS-protected envelope that can only be opened by an authorized recipient.

One of GigaTrust's first customers is the National Occupational Testing Institute, to keep people from copying tests, and also to protect their IP. It also has customers in the legal and healthcare markets.

Arizona-based **Informative Graphics Corporation** (IGC) has historically provided large format document (e.g. blueprints) management solutions primarily to companies in the manufacturing, architectural, engineering & construction markets. Today IGC also manages typical office documents, and supports integrations to ECM (Enterprise Content Management) vendors such as OpenText and EMC/Documentum.

Visual Rights™, a component DRM/ERM technology from IGC, is a layer that sits on top of DRM/ERM software, such as that from **SealedMedia** (more on SealedMedia below). Once a user has access to a document, Visual Rights controls what they can do with the document visually, and allows users to apply integrated and persistent security controls to drawings, documents and images during the publishing process. Sensitive fields can be redacted (blocked out) based on user permissions. Authorized use of a document can expire, and watermarks and banners can be displayed to reveal rights or copyrights.

IGC offers a PDF-like document format called CSF (Content Secured Format) for free. Unlike PDF though, CSF is a closed format. IGC also offers 3DF, to handle 3-D drawing outputs from CAD/CAM (computer aided design/ computer sided manufacturing) systems.

Visual Rights™ helps protect MS Office documents once they are checked out of a *Sharepoint Portal Server*, and the company is working toward integration with Microsoft's RMS server. "We'll ultimately offer a solution that manages all document types within an enterprise," says IGC CEO Gary Heath.

Liquid Machines, based in Waltham, MA, provides ERM solutions that persistently control information to help enterprises comply with external and internal mandates. *Document Control* is Liquid Machines' ERM product, which includes:

- User actions, auditable for compliance reporting;
- Instantly Changeable user rights, regardless of where the information is;
- Content protection that can be automatically enforced for persistent control;
- No required extra steps, as users continue to work in the native application (on/offline).

Information is encrypted and protected no matter where it is stored or how it is used, including email, portable storage, or IM and the policy or protections cannot be removed unless authorized. When the user *moves* information between documents, such as using the clipboard or Adobe® Acrobat Distiller, *the policy moves with the content*, ensuring the enterprise retains control of all protected information.

The enterprise defines and controls user privileges on protected content from a central policy server. If each policy change requires the document to be republished, the enterprise will be constantly searching for these existing files, not to mention the impossibility of changing files on permanent media such as CD-ROM. Multiple roles – or sets of users and privileges – can be defined for each policy to allow different users differing privileges. For example, accounting can print a document but engineering cannot and both groups can read and write.

The Liquid Machines client supports existing application versions and operating systems without requiring upgrades or plug-ins. The client is distributed using standard automated deployment tools (using MSI) or a web-based download. The server connects with Active Directory or LDAP to leverage existing users, groups and authentication. Information is encrypted using industry standards such as DES, AES and RSA. Policies are stored in a standard SQL database. Communication between the client and server occurs using XML over a secure SSL channel

Pinion Software is an ERM provider based in Austin, TX, that also handles large format and 3-D documents, and is positioned similarly to IGC. But the difference? “We’ve taken an Operating System level approach,” states VP of Product Strategy Kelly Looney. “And we believe we’re the only vendor to provide protections at the application *and* kernel level, which is important, otherwise this level is open to an attack,” he says.

Pinion was formed in 1998 as a spin-off of a firm with roots in the defense intelligence business, so roughly half of their revenues come from the Federal government. Many of their other customers in the private sector are implementing to meet compliance demands, (such as those from Sarbanes-Oxley), to secure executive communications.

Pinon *Secure Enterprise* consists of two main products:

- SecureMail™ - protects information sent by email in *MS Outlook* and *Lotus Notes* email content and attachments;
- SecureShare™ - secures content via web links, enforces authentication, and facilitates publication of content through simple user interface or programmatic interfaces. Also provides an administrative tool for managing and auditing content, users, and event logs.

SealedMedia CEO George Everhart states, “We believe that we’re the leading vendor in the E/DRM space in terms of software licenses. Our largest customer has 60,000 seats. So our software is enterprise tested and proven.” SealedMedia customers include The Financial Times, Congressional Quarterly, and AOL/ Time Warner.

Data originators have complete control over what recipients can do with the information. The focus of version 4.0, released in June, is ease-of-use. The user interface is consistent regardless of the type of document being protected, and documents may be “sealed” automatically, or just with a simple right click of the mouse.

SealedMedia supports many standard document formats such as *MS Outlook*, *Lotus Notes*, *MS Office* and also *Adobe® PDF* and HTML, in addition to multimedia formats.

Content is sealed independently of the right to access it and rights are stored on a network-accessible server within the organization. Sealed content can be freely distributed, since only those who have rights to unseal the content can access it. This also enables the user to easily restore their secured files after a PC repair or upgrade. Rights to read, print, amend, store and forward, before or after a particular time and to work offline for defined periods of time are set individually. Embargoed information, such as financial results, can be distributed in advance of their release, with rights being granted at the proper time.

EMC/ Documentum is a key Strategic Partner of SealedMedia in the Enterprise Content Management (ECM) marketplace. While EMC/Documentum *eRoom* enables knowledge workers to plan and execute project work and collaborate with extended enterprise teams, *Sealed eRoom* enables secure web-based collaboration. SealedMedia ensures that digital information remains persistently protected within the eRoom itself and when files are viewed or edited on remote desktops.

The future of the DRM/ERM market is very bright, due to market and geo-political trends. The role that standards will play has yet to be determined, but there is one sure thing: organizations will continue to deploy DRM/ERM software at a rapid pace to comply with regulations and policies, and to protect their vital information, wherever it may reside.

Robert Smallwood is a Partner with IMERGE Consulting and may be reached at Robert.Smallwood@IMERGEConsult.com.

(www.Adobe.com).
(www.AirZip.com)
(www.Authentica.com)
(www.ContentGuard.com)
(www.Documentum.com)
(www.DigitalContainers.com)
(www.GigaTrust.com)
(www.Infograph.com)
(www.LiquidMachines.com)
(www.Microsoft.com)
(www.Pinionsoftware.com)
(www.SealedMedia.com)