

# E-DRM Plugs ECM Security Gap

## IMERGE Consulting, Inc

---

Robert Smallwood

April 2008

Robert.smallwood@imergeconsult.com

As Appeared in KM World

www.imergeconsult.com

The gaping hole in security schemes of enterprise content management (ECM) systems is that few, if any, protections exist once the information is legitimately accessed. This confidential information, which may include price lists, legal documents, patented designs, blueprints, and reports, can often be printed, emailed or faxed 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 enterprise digital rights management (E-DRM) software, also known as Information Rights Management or Intelligent Rights Management (IRM). E-DRM/IRM software protects e-documents through their life cycles, both in internal and external use, and helps organizations: 1) track e-documents and email access across the enterprise, 2) protect proprietary and confidential data, 3) maintain client confidentiality and privacy, and, 4) comply with privacy laws and government regulations such as the U.S. Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and others.

ECM providers have been partnering with or snapping up E-DRM providers to address content security issues.

**EMC Corp.** acquired E-DRM provider Authentica in February 2006 and integrated Authentica's products to offer EMC Documentum IRM Services. The U.S. Presidential Daily Briefing, giving access to certain pages of the document to those with security access, is delivered using the solution.

Also in 2006, **Oracle** acquired ECM provider Stellent (which had acquired **SealedMedia**, a leader in the E-DRM market earlier that year). Oracle renamed the SealedMedia product line Oracle Information Rights Management (Oracle IRM). Oracle recently announced a key milestone: the millionth independent end-user download of Oracle IRM Desktop agent. Oracle IRM customers include *The Financial Times*, *Congressional Quarterly*, and AOL/Time Warner.

Other leading E-DRM providers include:

**Fasoo** of South Korea, which stepped up its entry into the U.S. market last year with the launch of an Enterprise DRM network appliance called XDRM. Although new to the United States, Fasoo has one of the highest annual product revenues of any DRM software concern worldwide, as well as possibly the largest aggregate (global) installed base in Enterprise DRM.

Arizona-based **Informative Graphics Corp.** (IGC) has historically provided large-format document (e.g., blueprints) management solutions primarily to companies in the manufacturing, architectural, engineering, and construction markets. Today IGC also manages typical office documents and supports integrations to enterprise content management vendors such as OpenText and Oracle. *Visual Rights*, a component E-DRM technology from IGC, is a layer that sits on top of E-DRM software, such as that from **Oracle/SealedMedia**. 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.

**Liquid Machines**, based in Waltham, Mass., provides E-DRM solutions that uniquely supports the use of multiple policy servers including Microsoft Rights Management Services (RMS). Their products can help support existing networks—from laptops, file shares, and USB storage to BlackBerry devices. Integration with one or more directory servers such as Microsoft Active Directory and Sun LDAP facilitates user administration. Major customers include Microsoft (used to enable the Microsoft Communications Protocol Program to securely license its intellectual property in electronic document format), Coming, Goldman Saks, and \$10 billion hedge fund Fairfield Greenwich Group.

**Modevity**, based in Westchester, Penn. (near Philadelphia), released Imperium in late 2007, a new E-DRM technology for corporate applications. Modevity has content management and streaming media product lines, particularly targeted to the pharmaceutical industry in the Pennsylvania/New Jersey area, where major U.S. suppliers are largely based.

**“Organizations are becoming more dependent on virtual communications technologies such as video streaming, as a part of their communications and marketing mix.**

**“However, moving these content items online exposes intellectual assets that must be protected and secured. E-DRM solutions allow content owners to manage and control the distribution of their on-demand rich media content.”**

**—Ira M. Weinstein,  
Senior analyst/partner, Wainhouse Research**

**Pinion Software** is an E-DRM provider based in Austin, Texas, that handles large-format and three-dimensional documents, and is positioned similarly to Informative Graphics. But the difference is they have taken an operating system-level approach, one of the only vendors to provide protections at the application and kernel level (as does Oracle IRM above), which is important, otherwise this level is open to an attack. 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.

### **Limitations of current e-document security**

Content and electronic document security today is really primarily perimeter security—securing the perimeters within which e-documents are stored, rather than securing e-documents directly. Documents and emails are somewhat secure while they remain within access-controlled perimeters, such as file system folders, email inboxes, content

management, or collaborative repositories, etc. But these documents and emails are also routinely used and stored on thousands of desktops, laptops, and mobile wireless devices—inside and outside the corporate firewall—from where they can be easily and untraceably opened, copied, and forwarded to anyone, anywhere.

E-DRM (or IRM) software is filling security needs in a global business environment of increasing collaboration, integration, alliances and cooperation with competitors, or “co-opetition.”

**Robert F. Smallwood** is a founding Partner of IMERGE Consulting and author of “Taming the Email Tiger,” available at <http://www.lulu.com/imergeconsulting>