

# Beyond DRM

## What Online Publishers Need to Know

Complimentary White Paper from Vitrium Systems

### DOCUMENT ABSTRACT

Online publishers need to protect their documents without making access to content unnecessarily complex. Many would also benefit from understanding their secondary – often unauthorized – readers. In this complimentary White Paper we explore:

- approaches to document security
- online content sharing and how to benefit from “pass-along”
- how to improve the reader experience
- ways to protect online documents while making the content more attractive to authorized readers

In discussing these issues, we hope to address the potential of online content sharing in a new way and help you to consider the opportunities that come with a focus on content – not document – security.

# TABLE OF CONTENTS

Introduction	2
Digital Rights Management Today	3
A Fine Balance: Security and Sharing	5
Creating a Positive Experience for Readers	6
Document Security Protects Value-Added Content	9
About Vitrium Systems	10

→ This exclusive document has been brought to you by Vitrium Systems - [www.vitrium.com](http://www.vitrium.com)

Please feel free to share it with your peers.

## INTRODUCTION

Most document security companies concern themselves solely with the prevention of unauthorized access to content. Online publishers, on the other hand, struggle to find the correct balance between document security and a satisfactory reader experience.

Recently, a new approach to document security has given online content publishers the ability to protect their content without adding unnecessary complexity to document access. This new approach can also make documents a rich source of insight into their readers.

In this white paper we examine some of the current approaches to Digital rights management (DRM) and the considerations for copyright holders striving to prevent the unauthorized duplication of their works. We review the issues surrounding online content sharing, how to create an ideal experience for readers and some of the unexpected benefits that can come from document security.

*DRM is a business of trade-offs. To create the highest levels of document security, many limits must be placed on readers. But to allow for the largest readership and widest document distribution, document security must be as user-friendly as possible.*

## DIGITAL RIGHTS MANAGEMENT TODAY

Digital rights management (DRM) – defined as any technology that limits access to digital media like e-Books, music and video – is not without controversy. There is a great deal of debate about whether any limitations should be put on content distribution in the age of the Internet. Controversy aside, document security is a pressing issue for online content publishers concerned not only with copyright protection but also with understanding their readership.

Simply put, DRM is about protecting documents from unauthorized access. As Gartner analyst Rich Mogull writes, “Data security is about protecting data from unauthorized access and unauthorized use after legitimate access. Data security is primarily focused on keeping bad people from good content and keeping trusted people from misusing good content (maliciously or otherwise).”<sup>1</sup>

Copyright owners struggle to find a balance between security and access issues. How best to keep unauthorized readers “out” and deter document misuse by authorized readers? DRM is a business of trade-offs. To create the highest levels of document security, many limits must be placed on readers. But to allow for the largest readership and widest document distribution, document security must be as user-friendly as possible.<sup>2</sup>

### File-level Security

Companies who sell documents online generally employ file-level security mechanisms, which unlock content through relatively light security mechanisms, including registration and authentication via web-forms and email. For companies who distribute content for “free,” (usually in exchange for information about the reader, that will be used for purposes such as market research), security is often limited to the front-end of a transaction - the potential reader must provide some personal information to obtain permission to access the content.

In both of these scenarios, the online documents do not contain highly confidential or otherwise secure information. Nevertheless, the information they contain is valuable and readers are willing to pay for, or submit information in exchange for, document access.

<sup>1</sup> Gartner, Inc, Organizations Must Employ Effective Data Security Strategies, Rich Mogull, 30 August 2005

<sup>2</sup> In this paper “document” refers to any type of content that can be protected in Adobe® Portable Document Format (PDF). This includes papers, books, research, regulatory codes and articles; rich media including video, film, and music; and premium content such as fonts, textual content, audio, video as well as interactive elements such as FLASH. PDF simply acts as the canvas upon which all this content is packaged, ensuring that rich copyrighted material is paid for or accessed by an authorized end consumer.

Most content creators are very familiar with the document security options available with Adobe® Portable Document Format (PDF). Access limits on PDF documents can be set at the document level by using passwords or simply restricting certain features, such as printing, text selection or editing. Once documents are unlocked, they can be read and most can be distributed freely to additional readers.

### Enterprise DRM

For some organizations for whom document security and control as documents flow within an organization are critical – such as financial institutions, government, or healthcare organizations – enterprise digital rights management (DRM) is the only solution. Enterprise DRM uses encryption to provide granular controls tied to the individual document. Unlike basic (file-level) encryption, enterprise DRM follows the object throughout its life cycle, but requires deep integration with the business infrastructure and applications, and may not work between different organizations. Example controls include read, edit, forward, copy, paste, delete or expire the file after a set time.<sup>3</sup>

Complex and expensive enterprise DRM solutions may be appropriate in a context where high levels of security are critical and a great many documents will be shared within a large group of readers. According to Gartner analyst Jay Heiser, “If there is a need to set up a workgroup that can control access to sensitive data without involving the system administrators, then DRM products are often the most effective and convenient protection. The greater the number of users or documents, the more desirable DRM becomes.”<sup>4</sup>

For most companies, there are few choices in approach. Concerns about the relative weakness of file-based encryption has created an increasing interest in enterprise DRM systems. However, these solutions are costly, complex and do not allow for the widespread redistribution of documents.

<sup>3</sup> Gartner, Inc, Organizations Must Employ Effective Data Security Strategies, Rich Mogull, 30 August 2005

<sup>4</sup> Gartner Inc, Responding to Audit Demands for File System, Encryption, Jay Heiser, 17 February 2006

*“I [think we need to] soften the rough edges of DRM – when publishers deem it necessary at all – so it becomes more of a gentle reminder, a way to help “keep honest people honest.”*

*Bill McCoy, GM,  
ePublishing, Adobe*

### **Online Content Readers Like to Share**

- **89% of adult Internet users share email content with others**
- **75% of them share it with up to six others**
- **77.8% of professionals who download white papers and case studies pass them on to colleagues**
- **75% of them save them for future use**

## **A FINE BALANCE: READERS WANT TO SHARE DOCUMENTS**

One thing is clear, online document readers have strong opinions about DRM and how much security is tolerable. Surveying comments on Adobe’s ePublishing blog recently, we found several interesting posts that reflect common attitudes to DRM. Bill McCoy, General Manager of the ePublishing Business at Adobe sums up the middle ground in this debate: “There needs to be enough [document security] for an average internet user to access the document.” He goes on to say, “I [think we need to] soften the rough edges of DRM – when publishers deem it necessary at all – so it becomes more of a gentle reminder, a way to help “keep honest people honest.”<sup>5</sup>

Security considerations are similar in the retail sector. We are all familiar with the systems used by stores to combat shoplifting. Product tags and alarms deter shoplifters and are of little or no inconvenience to honest shoppers. However, the more deterrents stores put in place, the more aggravation they cause their customers.

Unlike retailers, though, online publishers have a continued interest in controlling document use and access after they’ve authorized its use. When online publishers make their electronic content available, they effectively grant access to a purchaser whom they can’t be sure will use it as was intended once the transaction is completed.

People who download documents certainly like to share them. In a recent study of over 1,000 US Internet users, 89% of adult Internet users indicated that they share email content with others, with 75% sharing content with up to six other recipients.<sup>6</sup> In a study by Bitpipe Inc., an online content syndication firm, 77.8% of professionals who downloaded white papers and case studies reported that they passed them on to colleagues, and 75% of them saved them for future reference.<sup>7</sup>

Clearly, the distribution of digital content is seldom limited to its original, authorized users. While this is clearly a matter of concern for online publishers, it is also an opportunity - they stand to gain a great deal from understanding both the way their documents are shared and the people to whom they are redistributed. But how can publishers limit the use of content to authorized users while exploiting the potential benefits of document sharing?

<sup>5</sup> From the corporate weblog of Bill McCoy, General Manager, ePublishing Business, Adobe Systems Incorporated. Visit his blog at <http://blogs.adobe.com/billmccoy/>

<sup>6</sup> “Nearly 90% of Internet Users Share Content via E-mail,” Sharpe Partners press release, January 25, 2006

<sup>7</sup> “2004 Forbes.com and Bitpipe Study: Readership and Usage of White Papers and Case Studies by Corporate and IT Management,” co-sponsored by Forbes.com and Bitpipe, Inc., March 2004

*A document, like a book, is a collection of pages. Many document owners would benefit from being able to secure a document while leaving certain pages unprotected.*

### The Benefits of Content, Not Document Security

One consideration is the nature of document protection itself. Most document publishers protect the entire document. Once a document is secured, even if it can be passed from an authorized reader to an unauthorized reader, it is rendered useless – it can't be browsed or experienced in any way.

Document security can be handled differently. A document, like a book, is a collection of pages. Many document owners would benefit from being able to secure a document while leaving certain pages unprotected. With this approach, when readers receive a new document, they have access to enough content to decide whether or not to pay for access to the rest of the document. In this way, page-level document security actually enhances the experience of authorized and unauthorized readers by allowing re-distribution and sampling of documents.

Publishers, meanwhile, are saved the trouble of creating a separate, limited version of the document for marketing purposes. In addition, content security can further the document owners' business needs long after the documents themselves have been initially distributed. For example, they can learn more about their potential audience by embedding online surveys in parts of a document available to unauthorized readers.

*Due to the widespread availability of free information online, readers expect to be able to share the content they have and often measure the relative ease of access to new documents against documents with no DRM at all.*

### CREATING A POSITIVE READER EXPERIENCE

Due to the widespread availability of free information online, readers expect to be able to share the content they have and often measure the relative ease of access to new documents against documents with no DRM at all.

In this context, it is difficult to create document security systems that do not cause frustration among users. Document security, inexpertly applied, can quickly become a deterrent for readers, especially as many people often feel they can most-likely find the information they need from another, more accessible source.

For some content providers, leaving documents unprotected is simply not an option. Therefore, a balance must be struck between creating a positive experience for readers and maintaining document security. There are no set rules governing how best to do this - the balance will depend on the specific needs of different content providers and readers. Nevertheless, a few fundamental issues should be borne in mind.

## *Six Considerations for the Reader Experience*

### *1. Balance Reader Privacy vs. the Publisher's "Need" to Know*

Balance Reader Privacy vs. the Publisher's "Need" to Know  
Content publishers must find a balance between gathering information about the reader (in order to validate the reader's right to access the content) with the reader's right to only provide essential personal information. Many content publishers feel the allure of asking for additional data during a security transaction, but asking for more information than is necessary for the transaction can leave the reader feeling that security system is needlessly time-consuming and invasive.

### *2. Consider Content Persistence vs. Content Protection*

#### Consider Content Persistence vs. Content Protection

Unencrypted content can be widely and easily transferred. As discussed above, easily shared information is shared – and often. For the online content sharers in the study above, "The most popular content is humorous material, with 88% forwarding jokes or cartoons. The second most popular category is news (56%), followed by healthcare and medical information (32%), religious and spiritual material (30%), games (25%), business and personal finance information (24%), and sports/hobbies (24%)." <sup>8</sup>

### *3. Consider Document Protection vs. Infringing on Private Property*

While unprotected digital information can be freely shared, it is usually of less value than information from protected sources. Encrypted content, on the other hand, is only accessible for as long as the reader recalls how to unlock it and is therefore easily lost to posterity. We all know how easy it is to lose - or forget - usernames and passwords.

### *4. Understand the Reader's Use Patterns*

### *5. Understand Your Commitment to Maintaining the Reader Record*

#### Consider Document Protection vs. Infringing on Private Property

In 2005 the Sony CD copy protection scandal brought the controversy surrounding DRM right into the public view. In short, Sony/BMG created software which was silently installed when customers used their desktop computers to play music CDs. This opened security holes on the PCs, causing a range of serious problems. Sony/BMG faced many lawsuits and were forced to recall the affected CDs.

In this instance, a well-known corporation neglected to find a balance between copyright protection and consumer privacy. Specifically, they failed to realize that many consumers are reluctant to have proprietary software installed on their computers, particularly if it's done surreptitiously.

### *6. Implement a Tolerable Document Security Level*

#### Understand the Reader's Behavior

Readers often want to download a document on one computer and read it on another. For instance, a reader might need to have the document on a desktop at work but may also want to transfer it to a laptop for travel. With many DRM solutions, this is not possible and the user's attempts to access the document legitimately are impeded.

<sup>8</sup> "Nearly 90% of Internet Users Share Content via E-mail," Sharpe Partners press release, January 25, 2006

### Understand Your Commitment to Maintaining the Reader Record

How long is the document publisher obligated to maintain a record that the reader has authorized access to a document? Vendors and publishers must balance the need to keep systems simple and databases clean against readers' expectation that, once authorized access rights have been granted, they will persist for a reasonable period of time.

### Maintain a Tolerable Level of Document Security

All DRM is susceptible to circumvention. How much security is enough varies from application to application. A blogger responding to a recent post in the weblog of Adobe's Bill McCoy, General Manager, ePublishing Business sums up accepted wisdom about the effectiveness of DRM. Blogger Ben Trafford comments:

"Let's face it - any DRM can and will be hacked. DRM should be like the Club - it deters your basic thief from stealing my car, but doesn't stop me from driving. If more people could grasp this idea, we'd have a much happier world...and doubtlessly, a lot more eBooks on the digital shelves. It's a real pity that big business seems to think that strong DRM is anything but a burden to customers. The strongest DRM gets hacked all the time - and at about the same speed as weak DRM. The only difference between the two is that one is a pain for the customer, and the other...is not."<sup>9</sup>

What is at issue here is the common belief that DRM is "a pain for the customer." In this context, it is important that reader's feel that the level of security is balanced out by the perceived value of the document's content.

It is also vital that content owners understand readers' attitudes to online content sharing. They must not get "in the way" of the experience that consumers of online data expect to have, whilst still protecting their property. Each company must evaluate the approach that best fits the needs of its readership to ensure the widest possible readership, the most leads or the greatest revenue.

<sup>9</sup> [http://blogs.adobe.com/billmccoy/2006/06/ebook\\_pioneer\\_j.html#comments](http://blogs.adobe.com/billmccoy/2006/06/ebook_pioneer_j.html#comments)

*There are a number of, perhaps unexpected, benefits that both online publishers and their readers can obtain through a thoughtful approach to document security. The right approach can help add real value to online content.*

*Online content is not simply a digital version of a physical product - it has a whole unique range of potential value-added content. A well designed approach to DRM will protect this aspect of a document's content, ensuring that it is only available to authorized users.*

## DOCUMENT SECURITY PROTECTS VALUE-ADDED CONTENT

There are a number of, perhaps unexpected, benefits that both online publishers and their readers can obtain through a thoughtful approach to document security. The right approach can help add real value to online content.

Again, the example of retail is instructive here. Most stores invest extensively in the entire shopping experience. Advertising helps to bring shoppers into a retail outlet and the store's design can encourage them to stay. In addition, loyalty programs keep customers coming back, whilst helping the store to learn about the needs of its customers.

Likewise, software companies add value to their products through extensive customer support and regular updates. While it is easy to obtain software through illegitimate means, doing so prevents the user from having access to these desirable extras. Therefore, users are still willing to pay for the "real thing".

In the case of publishers, an author's raw manuscript is given added value through an extensive editorial process and attractive production values (layout, illustrations and so on). Online publishers of electronic documents can create even greater additional value by including features that could not exist in the physical realm, including automatic updates, search engines and links to supplementary data online.

Clearly, online content is not simply a digital version of a physical product - it has a whole unique range of potential value-added content. A well designed approach to DRM will protect this aspect of a document's content, ensuring that it is only available to authorized users - thereby helping readers feel it is worth paying for the real thing.

As in the case of retail loyalty programs, this value-added content can also be used to help online publishers with their market research. The interactive nature of online documents can provide benefits to the consumer that simultaneously help publishers learn more about their readers' preferences. This, in turn, allows content providers to continuously improve their products in line with their customers' needs.

In addition to all these benefits, it should be remembered that freely accessible information is fundamentally less reliable than that contained in documents that are copyright protected. Search engines and other online information sources take freely available content, index it and turn it into something usable by the reader. But checks are limited and do not generally extend to fact-verification. For online content creators, a great deal of resources are invested into the editorial process which produces a peer-reviewed, high quality final product.

*“... anonymity blocks credibility.” Randall Stross, New York Times, March 12, 2006*

Readers are prepared to pay for this high-value content but they also want the ease of use of that freely available information provides. DRM can be difficult to implement because it implies a compromise between the publisher and reader.

In a recent article in the New York Times, writer Randall Stross explored the issue of whether free online articles such as those found in Wikipedia can be judged as credible without knowing the author. Like DRM itself, Wikipedia is controversial. Founded in 2001, “the system rests upon the belief that a collectivity of unknown but enthusiastic individuals, by dint of sheer mass rather than possession of conventional credentials, can serve in the supervisory role of editor.” The article explores the challenges of this model to the credibility of its content, concluding with the thought: “...anonymity blocks credibility.”<sup>10</sup> Ultimately, he concludes, there needs to be some more restrictive process to grant final approval, or “feature article” status to more of the online encyclopedia’s contributions.

In focusing on the additional value they can offer with digital content, online publishers can distance themselves from the often inferior content that is freely accessible online. A well thought-out approach to document security would be an essential component of any serious attempt to do this.

<sup>10</sup> “Anonymous Source Is Not the Same as Open Source,” Randall Stross, March 12, 2006, nytimes.com

## ABOUT VITRIUM SYSTEMS

At Vitrium we take a fresh approach to document security. We understand that readers often want to share content and that publishers want to facilitate this insofar as it can help to expand their legitimate readership. While publishers don't want this redistribution of documents to infringe upon their ownership rights, they also don't want to make gaining access to documents so complex that it discourages legitimate use.

In general, digital rights management companies are concerned with security above all other things. As a result, their solutions - while highly secure - can be cumbersome to deploy, non-user friendly and challenging to implement, manage and maintain. Where content security is the foremost concern, such limitations may be acceptable but for organizations who produce or distribute content widely, concerns such as cost, complexity, accessibility and usability are just as important as security. For these kinds of companies, page-level security is the answer.

At Vitrium, we developed protectedpdf with the needs of both readers and document owners in mind. We protect content at the page level, not at the document level. This gives online publishers the flexibility to unlock select pages and grant potential readers controlled insight into content, without compromising overall document protection. Readers can even unlock additional pages from within a document itself, without having to leave to visit a shopping cart.

Online publishers can track not only the first reader's access but every other instance of document access. It's easy to embed optional surveys or forms directly within the document to encourage willing readers to share their insights. Publishers can grant and revoke reader rights, control printing, update or even digitally "shred" documents dynamically, all while the document is in the public realm. All this is possible with no proprietary software - all readers need to be able to access the content is Adobe® Reader® and an internet connection.

Contact Vitrium Systems today to learn more about our fresh approach to content - not document - security.

### **Vitrium Systems Inc.**

[www.vitrium.com](http://www.vitrium.com)

1-866-403-1500, press '2' (for sales)

+1-604-677-1500, press '2'

[sales@vitrium.com](mailto:sales@vitrium.com)