



E-DRM and Financial Services

Highlights

- Who is managing your information while it's in use on internal and external desktops ?
- Can financial services organizations afford to be compliant within a few hundred servers, but not on tens of thousands of desktops ?
- What are the benefits of extending information management to the desktop ?
- How SealedMedia E-DRM works
- Real world E-DRM case studies in Financial Services
- Useful checklist for organizations evaluating E-DRM

Extending information management to the desktop

Conventional information management solutions only secure, control and track enterprise information while it is stored unused within server-side repositories. By encrypting documents and emails E-DRM vendors such as SealedMedia can extend security, control and tracking out to information "in use" on end user desktops, inside and outside the firewall. With control over both server and desktop information lifecycles financial services organizations can securely embrace cost-effective digital information workflows while better complying with regulations regarding the security and integrity of digital records.

E-DRM and Information Management

Every financial services executive knows that their organization must manage increasing volumes of digital information, while complying with an ever stricter regulatory environment

But what does managing information really mean ?

A leading Information Lifecycle Management (ILM) vendor defines it as *"getting the maximum value from information at the lowest total cost, at every point in the information lifecycle"* where lifecycle stages include creation, collaboration, publication, archival and deletion.

Information management is usually taken to include:

- Managing the cost and availability of information via tiered storage, backup/restore, replication, distribution and failover.
- Information archival, retrieval and records management for regulatory compliance.
- Organizing information-intensive workflows via version control, indexing and search, metadata/classification, workflow automation, collaboration.
- Securing and tracking sensitive information to protect competitive advantage and intellectual property, and to comply with information integrity and privacy regulations.

Today almost all information management systems are limited to the portions of information lifecycle that occur on the server. This is remarkable since information may "live" on hundreds of servers within the organization, but it "works" on tens of thousands of desktops, inside your organization and on the desktops of partners, suppliers and customers.

You could ask yourself - what is the point of managing information on servers when it is essentially unmanaged when in use on remote desktops ?



Problems of unmanaged information on remote desktops

The fact that information is essentially unmanaged while in use on remote desktops undermines much investment in server-side information management systems. For example, financial services organizations are investing heavily in server-side compliance management systems, only to find that:

- **Sarbanes-Oxley (SOX section 404):** While financial spreadsheets are in use on remote desktops, even if they have only been distributed to those desktops for review, nothing prevents them from being falsified or accidentally or deliberately redistributed.
- **Gramm Leach Billey (GLB):** While personal customer information is routinely in use on desktops throughout a financial services organization, or the desktops of its outsourced contract employees, nothing safeguards it from being easily and untraceably redistributed. Current procedures merely harden network perimeters against external threats rather than defending against internal threats.
- **ISO 17799:** Without the ability to manage information in use on remote desktops financial services organizations attempting to comply with the information classification recommendations of ISO 17799 are constrained to paper policies that in practice can neither be enforced nor tracked.

Financial services organizations are also investing in server-side records management systems, only to find that they cannot reliably implement record retention policies involving the routine deletion of appropriately aged information. Deleting records from servers still leaves thousands of copies intact on remote desktops, resulting in open-ended business risk and costly trawls through desktops as part of litigation-led disclosure procedures.

Perhaps even more worryingly, the inability to manage information on remote desktops may preclude the introduction of cost-effective digital information workflows, such as virtual deal rooms based on web-based collaboration, because of the ease and untraceability with which information can be leaked from such systems.

Benefits of managing information on remote desktops

E-DRM extends many of the benefits of server-side information management to information “in use” on remote desktops, inside and outside the firewall:

- **Security** – E-DRM can extend server-side access controls to include information actually “in use” on remote desktops. Only authorized users can open and use E-DRM protected information on remote desktops, and that access can be revoked or changed at any time, regardless of where the information is being stored or used (see below - “How SealedMedia E-DRM works”).
- **Audit** – E-DRM can centrally track all end user access to information on remote desktops, even when the end users are offline (i.e. disconnected from the network), including end users outside the firewall.
- **Organization** – E-DRM indelibly links documents and emails on the desktop back to server-side repositories, enabling end users to locate up-to-date versions and related information.
- **Version control** – E-DRM can revoke access to out-of-date information in use on remote desktops and route end users to latest versions.

By extending management to include information in use on the thousands of desktops within a financial services organization (and its outsourcing suppliers) E-DRM can extend compliance to include the security, tracking and integrity of information on the desktop; can extend records management to the desktop by revoking access to expired desktop records; and can enable a host of cost-effective digital workflows such as web-based collaboration that would otherwise put at risk by the relative insecurity of the end user desktop environment.

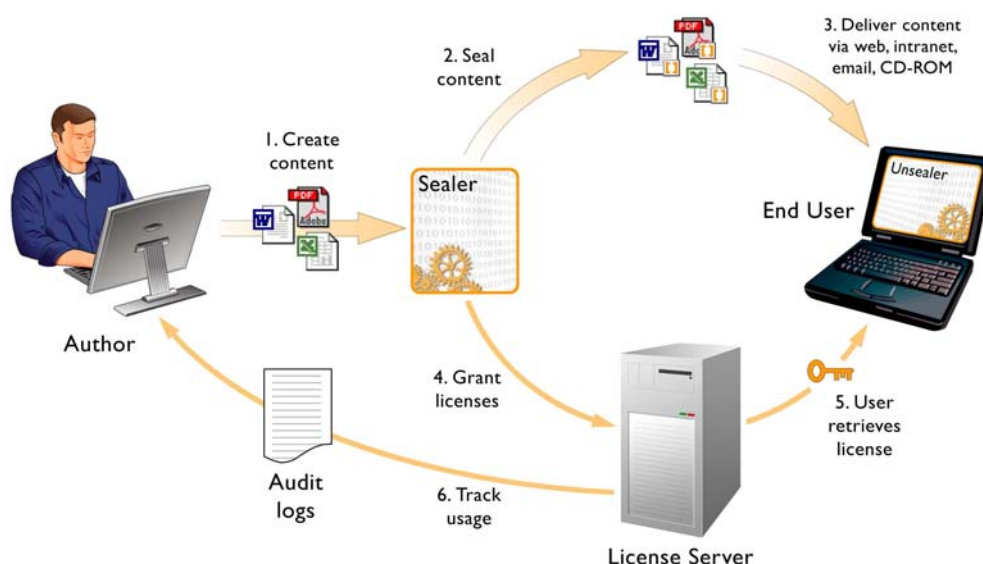


How SealedMedia E-DRM works

The fundamental ideas behind E-DRM are simple. E-DRM software is used to encrypt files so that only authorized users (who can obtain the decryption keys) can temporarily decrypt and use the encrypted files. The novelty of E-DRM, compared to previous encryption products, is in the transparency with which authorized users can use encrypted information within standard desktop applications and the fact that E-DRM client software continues to protect the encrypted information even while it is in use, preventing the end user from ever obtaining access to the raw, decrypted information.

The benefits of E-DRM apply wherever information is used, on desktops inside and outside the firewall:

- E-DRM server integration with existing authentication systems enables organization to enforce control over which users can access sensitive documents and emails on remote desktops.
- E-DRM client integration with desktop applications such as Microsoft Office, Adobe Reader and Lotus Notes enables fine-grained control (and tracking) of information use on remote desktops, such as printing, copying, annotation, editing, change tracking, interaction with form fields or cells, etc.
- The decryption keys and the associated end user access rights are kept safely on centralized, network-hosted E-DRM servers so that they can be revoked or updated at any time, on a per-user or per-file basis.



SealedMedia refers to the encryption and digital signing of files as “sealing”. As the figure above shows, SealedMedia E-DRM enables documents or emails to be sealed at any stage in their lifecycle, using sealing tools integrated into the Windows desktop, authoring applications, email clients and content management and collaborative repositories. Rights (licenses) can be assigned at the time of sealing, or separately, the latter being more typical in enterprise deployments where end users do not want to make rights management decisions every time they author a new document or email. SealedMedia only requires end users to install a single, universal E-DRM desktop application, known as the Unsealer, in order to both create and use sealed documents or emails in any of the 14 document and email formats currently supported. The SealedMedia Unsealer is responsible for authenticating the user, transparently requesting licenses from the License Server and protecting and tracking the sealed documents and emails while they are “in use” within their native applications.



Real-world case studies: Financial Services

The following 8 short case studies are all based on successful deployments of SealedMedia's E-DRM solution in some of the leading financial services companies in the world¹.

A leading equity hedge fund with over \$3billion under management

Much of the hedge fund's intellectual property resides in sophisticated Excel spreadsheets operating against live market data feeds from Reuters. The hedge fund used SealedMedia E-DRM to "seal" these Excel spreadsheets to protect their financial models from being taken to competitors by leaving staff.

Global investment manager with over \$92 billion under management.

The investment manager used SealedMedia E-DRM to "seal" its research for early viewing by a central bank, before release to normal clients worldwide. Access to the "sealed" research could then be reliably restricted to a select group within the central bank, protecting both the investment manager and central bank against the risk of illegal trading based on unfair access to market-moving research.

Prominent investor in the European buyout market whose latest fund closed at €4.4 billion

The investor used SealedMedia E-DRM to "seal" information and updates supplied to its investors via its extranet, to ensure that the investors do not re-distribute it, accidentally or otherwise.

Independent research firm providing specialized services to institutional investors

Under increasing scrutiny from the government and the SEC, and with the threat of regulation looming, the Investment Research industry is attempting to move towards a clearer model in which institutions pay independent research firms for research. The research firm uses SealedMedia E-DRM to control the circulation of its research, and to track illicit redistribution, thereby preserving its own revenue streams.

One of the UK's leading mutual societies

The mutual society uses SealedMedia E-DRM to prevent leakage of the terms of large commercial property deals to competitors by brokers; to protect sensitive information provided to the mutual society by its clients, as well as their own private analyses of client credit worthiness; to protect sensitive information exchanged with joint venture partners; and to protect personal customer information.

Leading re-insurance company with premium income in excess of \$30 billion

The re-insurance company uses SealedMedia E-DRM to "seal" the detailed financial and statistical analyses used to identify trends and adjust premiums, so that it can share it widely amongst its field staff. This empowers the field staff to act from a position of strength and knowledge, but alleviates the risk that the information will fall into the wrong hands and undermine the business.

Leading pension provider, subsidiary of one of the world's leading financial services groups

The pension provider uses SealedMedia E-DRM to seal Executive Management documents and emails, particularly when conducting top-secret negotiations for acquisition and divestment.

World leader in private equity and venture capital

The private equity company uses SealedMedia E-DRM to "seal" confidential information that it provides to its institutional investors to ensure that it can control disclosure in the face of US Public Information Acts.

¹ Note: SealedMedia has not named the financial services companies as companies often do not want to publicise their use of specific security technologies. For more information please contact SealedMedia sales.



Evaluating E-DRM solutions

While E-DRM may be conceptually straightforward, implementing it in such a way that it can be successfully deployed, used and managed within mission-critical enterprise environments is more difficult. The success of enterprise E-DRM projects rely on the degree to which the E-DRM vendors solution can address three key requirements:

- **Security** – The E-DRM solution must provide a reasonable degree of security against accidental or malicious abuse by end users of information.
- **Usability** – While being reasonably secure the E-DRM solution must not interfere with the day-to-day usability of desktop applications such as Microsoft Office, Adobe Reader and Lotus Notes.
- **Manageability** – The E-DRM solution must remain manageable by business process owners and IT administrators when used by tens of thousands of users, and for millions of documents and emails, circulating inside and outside the enterprise.

The checklist below explains some of the most insightful questions to ask E-DRM vendors:

Checklist	Explanation	Things to look out for ...
Deployments vs. Hype	E-DRM is a highly complex technology “under the hood”, which means that no feature comparisons or demonstrations can substitute for referenceable, successful, enterprise-scale deployments of the E-DRM solution in your industry vertical.	<p>Small-scale pilots vs. large-scale deployments. Many usability and manageability problems simply don't show up in small-scale and low-volume pilots</p> <p>Reference customers using product A, while you are buying product B. E-DRM solutions are often sold alongside other solutions, such as email or PDF security. Make sure to compare apples with apples !</p> <p>E-DRM solutions with immature and unproven product components, integrating with highly complex desktop applications such as Microsoft Office.</p>
Platform support	Your organization or department may all be running the same, modern versions of desktop application and operating systems but you will inevitably need to share sensitive E-DRM protected documents and emails with partners, suppliers, customers, acquired organizations, etc. over whose computing platforms you have little control or familiarity. Applications and operating systems have extraordinary longevity (6-8 years from release).	<p>E-DRM solutions that only support a narrow range of desktop applications and operating systems and a shallow range of the recent versions.</p> <p>E-DRM solutions where access rights are determined more by application and version than by policy, for example where users of modern application versions can edit encrypted documents, but users of older versions can only read.</p>



Checklist	Explanation	Things to look out for ...
E-DRM client deployability	The required presence of E-DRM client software on every desktop is what gives E-DRM its power to control and track information in use on remote desktops, but these benefits can be lost if the E-DRM client software is difficult to install, use and manage.	<p>Solutions that require users to install and use multiple E-DRM software components on the desktop, either because each E-DRM component is integrated with different desktop applications or different components are required for encrypting and decrypting.</p> <p>Solutions that require end users to have elevated administrator privileges in order to install E-DRM applications.</p>
Mobile/offline working <i>Note: Few things illustrate the complex, real-world balance required between security, usability & manageability than different E-DRM vendors' support for offline working.</i>	<p>Mobile users must be able to use encrypted information while offline, but this conflicts with the requirement to store access rights on centralized, network-hosted E-DRM servers in order to be able to revoke access rights after information has been distributed to remote desktops.</p> <p>E-DRM solutions must use sophisticated caching and automated synchronization of rights between E-DRM server and desktop in order to enable offline working without sacrificing timely revocation of information on remote desktops.</p>	<p>E-DRM solutions that require end users to guess which encrypted documents and emails they intend to use while offline, and to manually request offline "leases".</p> <p>E-DRM solutions that issue licenses on a per-file basis, making it impossible to synchronize those licenses to the desktop as the number of files increases, and therefore to have both offline working and revocation (you can have one or the other).</p> <p>E-DRM solutions that request per-file licenses from the server on first use, which fails to support the common use case of emails and attachments obtained while online but first used while offline.</p>
Classification-based vs. file-based	<p>It is impossible to manage large volumes of information on a file-by-file basis, so most enterprises have initiatives that "classify" information based on relative requirements for security, availability, retention, etc.</p> <p>E-DRM solutions must manage access rights at the level of easily understandable classifications such as RESTRICTED or CONFIDENTIAL (while easily making per-file exceptions) so that E-DRM can support and enforce document classification, and because attempting to support and enforce enterprise-wide policies on the basis of millions of per-file decisions is both impractical and undesirable.</p>	<p>E-DRM solutions that attempt to enforce document classification using complex Windows NT-style access control lists (ACLs), which can neither be managed nor comprehended by business process owners or end users.</p> <p>E-DRM solutions that issue per-file licenses from "templates" and then position the templates as supporting enterprise information classifications. The fact that per-file licenses are still issued "under the hood" then prevents these licenses from being synchronized to the desktop (as file volumes grow), meaning that either licenses cannot be revoked/updated (and only reflect enterprise policy at the time they were issued) or cannot support offline working.</p>



Summary

Financial services organizations are enormous users of digital information, much of which is highly sensitive, vulnerable to internal and external threats, and subject to compliance within an ever stricter regulatory regime. This situation is not helped by the fact that current information management systems leave off at the server, leaving the majority of information in use on internal and external desktops insecure, untracked and vulnerable. This whitepaper has discussed how E-DRM solutions such as SealedMedia can extend many of the benefits of server-side information management systems out to the remote desktops, inside and outside their organization, enabling financial services organizations to improve the security and auditability of their valuable information resources, to securely embrace cost-effective digital information workflows and comply with regulations regarding the security and integrity of digital records.

System Requirements

Unsealer

Windows 95, 98, 98 SE, ME, NT4.0, 2000, XP, 2003

License Server

Microsoft Windows 2000 Server or Advanced Server SP2
Microsoft Windows 2003

Database

Microsoft SQL Server 2000 or Oracle9i (on Microsoft Windows 2000 and Solaris 8)

License Server integration APIs

C++ and Java bindings on Microsoft Windows 2000, Windows 2003 and Solaris 8
Native COM binding on Windows 2000 and 2003

LDAP Gateway

Windows 2000 (Professional or Server), Windows XP, Windows 2003
Active Directory, iPlanet Directory server

License Server Event Messaging

Optional: MSMQ (option available with Windows 2000 and 2003)



Further Information

For more information about SealedMedia's E-DRM products, solutions and services:

- Please visit our web site at www.sealedmedia.com
- Or contact us directly:

US: +1 781 419 2650
us.info@sealedmedia.com

Europe: +44 1494 687200
europe.info@sealedmedia.com

© 2005 SealedMedia.
All rights reserved.
All trademarks acknowledged.
SealedMedia is a US Registered Trademark of SealedMedia Inc.

Published: February 2005