FileOpen for Corporate Enterprise Rights Management (ERM)

Corporations clearly need to secure proprietary or confidential information within their enterprise, and have many security schemes at their disposal to do so. But large-scale ERM (Enterprise Rights Management Systems) aren't a good fit for two common scenarios.

First, a smaller business or unit within a corporation may need to quickly control a set of documents without having to implement an enterprise-wide document management system. Second, corporations frequently need to share confidential documents with partners and contractors outside their firewall, and want the same degree of protection for those users out in the field.

An effective document control system for the corporate enterprise must be able to handle these scenarios, in addition to the basic requirement of preventing document leakage out of the firewall. Securing documents in a corporate setting also carries a unique set of requirements (as distinct from mass-market document publishing):

- Access to documents should be tied to existing login credentials to enable dynamic granting and revocation of permissions based on user's role in the organization.

- Encryption of documents should be dynamic (e.g. watched directory) and support a high volume

- Any client software or plug-in must be remotely and automatically installed without requiring high-level administrator privileges

- The system should leverage existing document creation and security systems

- The system should support internal document review methods, fill-in forms, digital signatures, etc.

- The system should be able to support BYOD (Bring Your Own Device) for access from personal laptops, iPads and smartphones

The FileOpen Approach to Enterprise Document Control

FileOpen document control takes a modular approach that enables corporate users to add a layer of security to their existing firewall. Files may be encrypted either on a

central server or on the desktop. Authentication may be tied to existing login credentials or new criteria—users and/or documents may be grouped for selective access. User data can be stored in the FileOpen RightsManager's cloud-based database, or integrated with the corporation's own database (e.g. LDAP). The FileOpen system has an open protocol for easy integration with existing CMS and document management solutions, but does not require such systems to operate.

The flexibility of the FileOpen approach extends to the recipients of secure documents, the end-users. The client plug-in to view secured files may be installed remotely and automatically to all recipient desktops, installed via email, or obtained directly from the Web. Depending on the file formats and security settings chosen by the document owner, the end-user may access secure files from the full spectrum of platforms and browsers, online and/or offline, and also from their handheld device. They may print the document at the owner's discretion (dynamic watermarking is available to stamp user data on printouts).

A few examples of FileOpen Enterprise Customer Implementations[1]

Internal Document Control using FileOpen RightsServer™:
A global designer of luxury goods with over 3 billion in annual revenues needed to secure their sales reports, with the requirement that the reports be viewed only by certain recipients within the company, and under no circumstances be accessed outside the company firewall.

Using FileOpen RightsServer, the company integrated the FileOpen Encryptor module with their automated workflow system, which produces PDF versions of the reports. The PDFs are automatically encrypted at the end of the workflow and dynamically watermarked with the name of the recipient, before being routed to their desktops. The encrypted documents are also sent to an automated printing system which imposes the watermarks for an auditable paper trail. The files are set to print only on the authorized printer.

The result: The Company was able to "bolt on" the FileOpen encryption function to their existing document workflow, with no need to convert file formats. Using FileOpen RightsServer, managers can grant or revoke access to specific users, even after delivery. They are able to tightly control printing to a single internal device, with the added assurance of identifiable watermarks on printouts. Authorized recipients may view the encrypted files in the normal Adobe Reader with no password entry required. Should

---

[1]   The following examples are based on real implementations by existing FileOpen licensees. Their names have been withheld to protect their business practices.

one of the PDFs make its way to another desktop or outside the firewall, it cannot be opened by any other user.

Internal/External Document Control using FileOpen client/server implementation:

A top-ten hedge fund with $14 billion in assets under management needed to distribute confidential financial data within the company and also to a small subset of their limited partners outside the firm. Maintaining the security and integrity of the documents was a top priority, particularly for the documents being distributed outside the firewall. At the same time, the hedge fund managers did not want to complicate access for its partners, or embark on a large-scale implementation with their small IT staff.

The hedge fund chose the FileOpen RightsServer and RightsManager products with PDF Control, because it would give them the most flexibility in implementation. They decided to address the problem in two phases, starting with internal document security as Phase 1 and progressing to external distribution in Phase 2.

In Phase 1, the firm installed the FileOpen RightsServer on an internal Web server and enabled a selected group of managers to encrypt and distribute secured documents. The managers used the FileOpen user interface to selectively grant access to the documents within the firm.

Once Phase 1 proved successful, the firm deployed the FileOpen RightsManager, a cloud-based authentication server, to handle user authentication for documents distributed to their limited partners outside the firm. While their internal FileOpen RightsServer could have performed authentication of outside users, the firm preferred not to have any outside traffic within their firewall. FileOpen RightsManager gave them the option to continue to use the same user interface to encrypt and distribute documents, but have external authentication requests handled by an outside secure server. For an additional layer of security on the documents, the firm sends to their outside partners, they opted to make the documents read-only and disallow printing. Because the files are PDF and display in the Adobe Reader, their limited partners only needed to authenticate once to obtain their permissions and the client plug-in. The plug-in will silently communicate with the FileOpen RightsManager to check the user's credentials for every new document that arrives, with no password entry necessary.

The result: The hedge fund was able to seamlessly blend two FileOpen solutions to secure their sensitive financial data both internally and externally. Using two separate authentication servers, the hedge fund managers can be absolutely certain that no outside users can cross their firewall, and that documents outside the firewall are persistently secured.

External Document Control using the zero-client install FileOpen Viewer:

A Wall Street investment firm wanted to switch from sending confidential financial data to its clients as PDF email attachments, to posting them on a secured portal on their web server. They wanted a high degree of security, but without the administrative overhead of distributing a client plug-in to their users outside the company firewall, since they could not control the end-user environment. Although it is difficult to match a high degree of security with the requirement of no client software, FileOpen had a solution.

FileOpen demonstrated its FileOpen Viewer™ system to the investment firm, which converts standard PDF files to OPN format and displays them in any Web browser running Adobe Flash Player with no client plug-in. The firm implemented the system so that only registered portal users can view the files, and no local copies can be saved. They allow printing of the encrypted documents, but they are watermarked with the user's ID so that printouts can be traced back to the user and printer. If an encrypted OPN file somehow escapes the firewall, an unauthorized user will not be able to open it, even if they obtain the OPN viewer.

The result: The investment firm implemented a highly secure document portal without the need to push any software out to end-users. They can be certain that their authorized users won't have access problems, since OPN files can be viewed on any system that has Adobe Flash. The OPN files viewed by the end-users are printable, vector files that appear and behave in every respect like the source PDF file, with the addition of optional watermarks.

Licensing Options for Enterprise Customers

- FileOpen RightsManager: Recommended for customers who wish to encrypt documents locally but prefer to authenticate via an FileOpen's server

- FileOpen RightsServer: Recommended for environments running standard Windows server platform, to keep all server functions within the firewall

- FileOpen Developer Toolkit: Recommended for IT departments running non-Windows platforms (e.g. Java). Can be tightly integrated with existing database and authentication systems

Conclusion

FileOpen's solutions give enterprise customers the flexibility to quickly integrate document security with their existing systems. These solutions are available as separate

modules or as a hosted service, offering the features of a large-scale ERM system without the commitment of IT resources those systems require.