WhitePaper

FileOpen for Secure Virtual Data Rooms (VDRs)

What is a Virtual Data Room?

A Virtual Data Room ("VDR") is a virtual space for sharing documents, most often of a legal or financial nature, among the parties to a transaction who are accessing it remotely from diverse locations. VDRs use a high level of perimeter security and are designed for temporary access and document review by an ever-changing roster of users. In recent years, VDRs have gained in popularity as a way to reduce the need for traveling to a physical location to negotiate a deal, with the associated legal and printing costs.

VDRs Standardize on FileOpen Document Control

A number of vendors have established a market for outsourced VDR technology, providing the secure servers and document management technology to clients who don't have the desire or technical resources to host their own data rooms. Many of these VDR vendors have licensed FileOpen RightsServer™ to encrypt documents shared in their data rooms, such as Intralinks® Virtual Data Room, Investran SunGard DX, Imprima iRooms, Firmex, Pandesa, EthosData, HighQ Solutions, Real Capital Markets, V-Rooms, Transperfect Deal Interactive™ and SmartRoom™ by BMC Group Inc.

Do-It-Yourself VDR

FileOpen Systems will also license tools directly to law firms, investment firms, and other entities so they can host their own secure dataroom. FileOpen's document control solutions are particularly well-suited to the unique requirements of VDRs, namely:

- Users must be able to access documents in the VDR remotely, from a variety of platforms and user environments
- Any client software installation must pose the absolute minimum inconvenience to end-users
- The VDR documents must be strongly encrypted to prevent unauthorized viewing, and be encrypted in real-time as they are delivered, or ahead-of-time in batch when placed in a watched directory

- Permissions must be dynamically imposed, allowing for revocation after delivery, and allow for quick inclusion new VDR participants
- Document access should be seamless once a user has authenticated and entered the dataroom, without having to enter document-specific passwords
- The system must support fine-tuned access controls such as restricted printing, watermarking, and expiration of privileges
- The encryption must not interfere with document review and digital signature tools

The FileOpen Approach

The FileOpen Encryptor, whether hosted by FileOpen or installed on the VDR's server, is engineered to dynamically encrypt any volume of files in a watched directory, and can impose unique watermarks with user data, time and date, etc. Watermarking is especially useful in the case of VDRs, since they can aid in tracking and version control of printed documents.

The FileOpen RightsServer™, also available in either a hosted or licensed implementation, offers highly granular access controls, such as document expiration after a period of days, hours or even seconds, and page-level control over viewing and printing. The RightsServer™ may be linked to the host's user database and firewall authentication, so that any change in credentials can be enforced on documents, even after delivery to the user. These access controls not only increase the security of VDR documents but enable version control, ensuring that users are always working with the most current version of a document.

Authorized end-users can access the secure documents seamlessly (without passwords) as long as they are logged into the VDR's server or using an authorized machine. In most cases, users may view the secure files natively in the familiar Adobe Reader interface, or take advantage of the markup, review and digital signature tools in Adobe Acrobat Pro. If offline permission is granted by the VDR, the user may access the document while disconnected from the Internet, e.g. on an airplane. Because FileOpen client software uses only standard encryption methods, file formats, and ports for communication with the server, authorized users are unlikely to experience problems accessing their documents.

Up and running in two days

A boutique investment firm recently approached FileOpen Systems with an urgent need for an in-house secure VDR. The firm wanted a solution that would enable a quick implementation with no installation of software at the user end.

FileOpen suggested they use FileOpen's Developer Toolkit with FileOpen Viewer, which offers a high degree of security along with no client software requirement. Using example code provided by FileOpen, the firm's small IT staff configured their own Windows-based permissioning server to handle dynamic user access inside the VDR. The firm opted for the highest degree of access control on the encrypted documents — viewable only online while logged in to the VDR, no saving allowed, no printing allowed.

There was no need to push any client software out on to their users, because the FileOpen Viewer works on any platform and browser where Adobe Flash is running, representing over 98% of systems. The look and feel of the documents closely resembles the source PDF files, giving end-users an easily navigable and crisp rendering of the document.

The Result: Within two days of licensing modules from the FileOpen Developer Toolkit, the boutique investment firm had a working dataroom up and running.

FileOpen Rights Management: The Solution for Secure Dealrooms

Whether they choose a hosted or licensed solution from FileOpen Systems, VDR hosts have the option of distributing documents in native PDF, the plugin-free OPN format, and the MS Office formats (Word, Excel, and PowerPoint). FileOpen-encrypted documents can even be viewed on users' iPads and iPhones. VDRs hosts may pick and choose among the wide range of options in the FileOpen product line to create a customized VDR quickly and effectively.