10 Ways ShareVault Secures Confidential Documents Better Than Anyone Else

ShareVault customers are often impressed by the extent to which ShareVault is able to secure and protect their content, but also by just how easy ShareVault makes it to enforce these ultra-secure policies. Remember, when you're sharing documents with third parties, your documents will be accessed on computers over which your IT department has no control. It's therefore important to note that not all data rooms are created equal. To rest easy knowing your most confidential documents are secure, insist that your data room has the following features:

#1 GRANULAR PERMISSIONING

Permissioning is defining who has the rights to see which documents in the data room. Permissions can be set at the group or folder level which makes it quick and easy to set permissions for many users across large groups of documents. But ShareVault also supports permission overrides, which can be applied at the user and/or document level so you can handle special cases with ease. With ShareVault it's extremely quick and easy to set up permissions and also to make changes to the permissioning for staging. Staging, or the ability to modify permissions as your project progresses through phases of increasing trust with the other party, is a very important capability for a solution such as this.

#2 CUSTOMIZABLE DOCUMENT SECURITY POLICIES

Permissions are basically an on/off switch. In other words, a user either has permission to access a document or not. The next question to address is what a user having permission to a document can do with that document. That's where policies come into play. Most secure sharing platforms that allow for policies are limited to just view, print and save. But with ShareVault policies are fully customizable. ShareVault lets you select from seven security attributes and allows for batch operations so you can easily stage your polices as your trust with the other party increases. For example, you might want to grant users the right to print certain documents as the project moves into later stages.

#3 DYNAMIC WATER-MARKING

Watermarks provide a simple, yet effective, security

mechanism. ShareVault applies customized dynamic watermarks automatically to every page of a document. If you allow users to print documents, watermarks provide a strong deterrent against circulating the printed documents because the user's identity is shown in large text diagonally across every page of a document in a way that does not interfere with the readability of the underlying text. Watermarks are easy to configure and automatically change based on the identity of the end user who is currently viewing the document.

#4 SECURE PRINTING

In some cases the party with whom you're sharing documents will insist on being able to print. For example, lawyers in the later stages of a project will want printed copies of contracts to review, mark up and add notes. Knowing that the user could just print the document to PDF loses control over the electronic version of the document. ShareVault has a feature that provides for printing only to physical printers and blocks printing to PDF, Tiff and XPS, so you maintain control of the shared files. Without this feature, enabling printing is the same as allowing a document to be saved. ShareVault also has a powerful batch print feature.

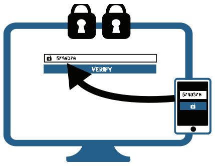
#5 REMOTE SHREDDING

Most ShareVault customers do not want users to be able to save documents. However, in some applications, the ability to save documents can significantly accelerate the review process. This is particularly true for very large documents such as clinical trial results which could be thousands of pages long. Our competition will recommend breaking large documents into smaller chunks, maybe hundreds of pages each, so reviewers don't have to load the document every time they want to open it to continue reading. With ShareVault, however, you can allow users to save those sensitive documents right to their hard drive so they can instantly open them whenever they want to continue reading. Then you can remotely shred those documents whenever you want. In other words, you can retroactively revoke a user's right to open a document even after they've downloaded it. ShareVault's powerful Secure Save technology is based on secure AES-256 encryption. To open a previously downloaded document a user has to be logged into ShareVault, has to still be a member of your ShareVault, and has to still have permission to that document. If any of those criteria are not met the document will not open. If the document is open when permission is revoked, the document will immediately close.

#6 SCREENSHOT BLOCKING

ShareVault prevents screenshots on both Mac and PCs not only using the native screen capture, but also third party screen capture products like SnagIt. ShareVault can also prevent screen sharing software such as GoToMeeting. If you're sharing your screen with someone else the other person won't be able to grab a screenshot. We even prevent screenshots on our iOS and Android apps.

#7 TWO-STEP VERIFICATION



You've probably encountered two-step verification, also referred to as two-factor authentication, on your bank's internet site or when logging into a Google account. A code is sent by text message to your phone, and you must use it in order to log in. ShareVault uses a similar approach. (For users who want to use ShareVault from locations without cell phone coverage, we are also compatible with Google Authenticator on iOS, Android, Windows Phone and Blackberry.) Information security experts generally consider two-factor verification a must-have security feature because it makes it so much harder for a hacker to gain unauthorized access to a site through an authorized, but hacked, user's account. To breach an account a hacker would not only need to know the user's password and security question, but would also have to gain access to the user's mobile phone.

#8 MULTI-LEVEL ENCRYPTION

With ShareVault your files are encrypted at each stage of the document's lifecycle. During upload and download files are encrypted in transit using 256-bit SSL encryption and while at rest using AES 256-bit encryption. As most information security experts know the most critical aspect of data security is the encryption key management. ShareVault's key management workflow ensures that only the intended ShareVault users can access your files. A person accessing the ShareVault back-end service is not able to open your files. This means that employees of ShareVault, or ShareVault data centers, are not able to access files. Even though all ShareVault employees have undergone background checks, information security auditors can rest assured that their data is protected even against rogue employees. And, as we've already discussed, ShareVault doesn't stop with encryption in transit

100,000 people in 48+ countries use ShareVault for unmatched document security

and encryption at rest. Documents saved with Secure Save technology also continue to be protected on your end user's computer. We call this persistent encryption provided by Secure Save, encryption "at the edge" so your content is protected through your project's entire lifecycle.

#9 SECURE AND RELIABLE CLOUD INFRA-STRUCTURE

ShareVault is available to all of your users worldwide because it's based in the cloud. We've invested heavily to ensure that ShareVault's infrastructure is both reliable (with a 99.99% uptime) but also hardened with audited best practices which provide the security that our customers expect from us, including the applicable certifications.

These include:

- High-availability architecture
- Geographic redundancy and failover
- Data center certifications SSAE-16 Type II, ISO 27001:2005 & HITRUST for HIPAA compliance
- GDPR compliant
- Skyhigh Enterprise-Ready
- Secure software development lifecycle
- Regular vulnerability scans
- Teridion data transfer performance

#10 CUSTOMER-MANAGED ENCRYPTION KEYS

Information security experts know how important customer-managed keys are for ultra-secure enterprise applications. Encryption keys are basically long, complex numbers kept in a secure, virtual vault in the cloud. Without the proper key the file cannot be decrypted. Only the intended users can view the content. Each time a key is retrieved from the vault and used it is immediately destroyed and never stored, except in the vault. The advantage to ShareVault's implementation of customer-managed keys is that, unlike our competitor that offers this advanced feature, it's completely transparent—there's no need for your IT department to get involved in setting up and managing a hardware security module.

Remember, a virtual data room can be an essential tool for facilitating deal transactions and other applications where it's imperative to share confidential documents securely. However, choosing the right virtual data room with the advanced functionality you require can be the difference between an efficiently streamlined process and one that is aggravating and compromises deal success.Find out more at www.sharevault.com.