



ShareFile Security Report

This whitepaper outlines many of the security and privacy measures that in place for the ShareFile system. ShareFile's security measures can be divided into three main categories: Servers, Software, and Policies.

Servers

ShareFile's servers are located in a facility that is managed by Hosted Solutions, a trusted provider of secure and reliable data centers.

The data center features the following security measures:

- Ballistic-proof exterior, including doors & windows
- Double Man Traps force double verification and provides extra secure data center entry
- Redundant off-site monitoring of all security systems
- Locked Cabinets and Cages
- Fingerprint scanners and ID checking for all entry and exit of the hosting facility

Additionally, ShareFile's servers are protected with a dedicated WatchGuard firewall, which constantly scans for and protects against malicious threats such as viruses, worms, spyware, trojans, spam, and blended threats. The firewall also provides 'zero day' protection against anything that does not conform to standard Internet protocols, behaviors, and patterns.

All servers are automatically updated with the latest security patches using the Windows Update service.

As a further security measure, ShareFile's servers are subject to weekly security audits by a third-party security monitoring firm.

Software

ShareFile's software has been created with security in mind. Each user of the system has a unique login and password. All user passwords are hashed in the ShareFile database, meaning that not even the ShareFile support personnel have the ability to determine a user's password.

ShareFile users can create folders in the system, and only specified users that are designated by owner of the folder are able to access the contents of the folder. Users who do not have access to the folder will not even see the folder in their view of the system.

If the 'Send a File' or 'Request a File' features are used instead of folders to quickly transmit files through an e-mail link, users always have the option to require login before downloading the files.

All communications between ShareFile and the user are encrypted using the Secure Socket Layer (SSL). This is the same functionality used by banks and popular e-commerce services such as Amazon.com for secure communication. All files are stored on the ShareFile servers using a 32-character random filename with no file extensions.

Policies

In addition to hardware and software measures, ShareFile also has several corporate policies in place to help protect the security of data in the ShareFile system.

While some access to client data is necessary in order to perform support functions, a random 32 character password must be provided in order to access any support functions in the ShareFile system. This password is changed frequently, and access is restricted by IP address so that support functions can only be performed from within the secure ShareFile physical office facilities.

Further, it is a company policy that ShareFile support engineers may only access client data when such support has been specifically requested by a user.

For any security questions not addresses in this document, please contact support@sharefile.com.