ShareFile
by CITRIX

FACT SHEET | Security

Security Report

The ShareFile system has many security and privacy measures in place to protect data. These security measures can be divided into four main categories: Software, Backups, Servers and Policies.

Software

ShareFile's software has been created with security in mind. Each user in the system has a unique login and password. All user-created passwords are hashed in the ShareFile database, meaning that not even ShareFile support personnel have the ability to determine a user's password. Granular access permissions allow users to be given access to information on an account on a need to know basis.

ShareFile has a daily third party security scan through McAfee® SECURE. The appearance of the McAfee® SECURE seal on our login page indicates that ShareFile has passed the security audit. If McAfee® SECURE ever finds an alert that causes us to fail the security audit, the seal will temporarily disappear until the security hole is repaired.

All uploaded files are scanned by anti-virus software. Any files that are flagged as potential viruses are denoted with a red exclamation point icon within the application, and a warning will be displayed before attempting to download these files.

All communications between ShareFile and the user are encrypted using either Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption protocols and up to AES 256-bit encryption. This is the same industry-standard protocol used by online banking and popular e-commerce services such as Amazon.com for secure communication over the internet. Files at rest are also stored using AES 256-bit encryption.

Backups

ShareFile employs multiple backup measures to minimize data loss in the event of natural disaster, terrorism, fire or any other unexpected event that could result in the destruction of the hardware that hosts the service.

Disaster Recovery

Client files are backed up to ShareFile's disaster recovery data center every four hours. All client files are mirrored in real time to multiple storage zones. In the event of a failure in the primary storage zone, the secondary zone within that region is used automatically. In the event of a natural disaster or catastrophic hardware failure at the primary data center that services an account, resources at the disaster recovery data center can be brought online to minimize the disruption to the service.

Redundant File Storage

ShareFile maintains the capability to leverage alternate regions to store files if any one region is rendered unavailable. Additionally, ShareFile maintains a geographically separate backup and file recovery site that provides it the capability to recover a client files in case of accidental client-side file deletion. All client files are backed up to our alternate site within four hours of initial upload time.

Lazy File Deletion

To protect against the accidental deletion of files, ShareFile maintains copies of all deleted files for 28 days total before permanently purging the files from the backup and file recovery center. This helps protect clients from file loss due to user error. If a file is deleted in error, the file can be restored through ShareFile's Recycle Bin feature.

Servers

Each of ShareFile's data centers has attained third-party SSAE 16 Type II certification, which verifies all data center facilities operate with strict security procedures. Physical access is strictly controlled at the perimeter and building entrance points, and access to each data center is accessed with two-factor authorization.

Additionally, ShareFile's servers are protected by dedicated firewalls, which constantly scan for and protect against malicious threats. The firewalls provide zero-day protection against any traffic that does not conform to standard Internet protocols, behaviors or patterns.

All of ShareFile's servers are automatically updated with the latest vendor-supplied security patches for the operating system and other applications.

Policies

ShareFile also has several corporate policies in place to help protect the security of data in the ShareFile system. All support functions are conducted by ShareFile employees, and access is restricted by IP address so that support functions can only be performed from within the secure ShareFile physical office facilities.

Furthermore, it is a company policy that ShareFile support engineers may only access client data when such support has been specifically requested by a user. All login and upload/download activity by ShareFile support engineers is logged in our system activity log, which is fully viewable by administrators on each account.

In addition to hardware and software policies, ShareFile also maintains a business liability insurance policy to protect the company and its clients against any data loss.

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