memeo

Memeo Send Security

Memeo Send is a new web service that allows users to securely send large files over the internet. Memeo utilizes different technologies and infrastructure to ensure that your files are sent safely and securely.

The Memeo Send client communicates with the Memeo Send servers using industry standard secure protocols. There are three different paths by which our client communicates to the server:

- **Login -** For login authentication, we use OAUTH, an open protocol that allows secure API authorization. OAUTH is also used by leading web service companies such as Twitter, Flickr and Google.

- **File Send/Receive -** Files are uploaded and downloaded using 128-bit SSL connections. This ensures the connection is encrypted and secure.

- **API -** The client communicates to the servers for updates and status using 128-bit SSL. This ensures that this communication is done over an encrypted pipe.

Files downloaded via the web browser client utilize a 128-bit SSL connection over https. This will encrypt the connection so that it remains secure from end-to-end.

Files that are sent via Memeo Send are kept on our servers for two weeks. After this, they are deleted. If a file or set of files has not been downloaded in this window, we require them to be resent. This means that your data ends up only with the people that you want to have the files.

The Memeo Send servers are housed in a secure, fault-tolerant data center in the heart of Silicon Valley, CA. Access to the datacenter is restricted to qualified Memeo personnel only.

Memeo datacenters are equipped with redundant power from separate grids, redundant cooling systems, as well as multiple fiber links in and out of the facility. Diesel generators capable of running for an entire week, back up the entire facility in case of catastrophic power loss.

Memeo also has emergency recovery plans in place which assure full recovery and operability within 72 hours in case of a major catastrophic event.