Security

Last modified: March 28th, 2018

Security Overview

We provide this overview so that you can better understand the security measures we've put in place to protect the information that you transmit using Mover.

Secure Storage & Transfers

We encrypt the files that you transmit through Mover using the AES-256 standard, which is the same encryption standard used by banks to secure customer data. Encryption for your files is applied as soon we receive them, and we manage the encryption keys.

Mover uses Amazon EC2, Microsoft Azure, Google Cloud Compute, and other custom hosted servers for our server infrastructure. Microsoft, Google, and Amazon store data over several large-scale data centers.

You can find more information about:

- Amazon's security at the Amazon Web Services' website.
- Google's security on the Google Cloud Platform website.
- Microsoft's security at the Microsoft Azure website.

If supported, your files are sent between the services you choose and our servers over a secure channel using 256-bit TLS (Transport Layer Security) encryption, the standard for secure Internet network connections.

Your Data is Not Retained by Mover

After we have completed transmission of your data between the services you have directed us to use we remove any copies of your data from our servers. We simply facilitate the transfer of your data and we have no interest in, or benefit from, retaining your data.

Privacy

We guard your privacy to the best of our ability and work hard to protect your information from unauthorized access.

Mover employees are prohibited from viewing the content of files you transmit through Mover, and are only permitted to view file metadata (e.g., file names and locations). Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.

On the rare occasion, Mover employees may access your connections and files only to fix bugs or troubleshoot problems that have been identified.

Compliance With Laws and Law Enforcement

As set forth in our privacy policy, and in compliance with Canadian law, Mover cooperates with Canadian law enforcement when it receives valid legal process, which may require Mover to provide the contents of files we currently possess. In these cases, Mover will remove Mover's encryption from the files before providing them to law enforcement. Since we do not retain any files after their transmission it is highly unlikely that we will have any of your personal data on hand if such a legal request occurs.

How to Add Your Own Layer of Encryption to Mover

Mover applies encryption to your files after they have been uploaded, and we manage the encryption keys. Users who wish to manage their own encryption keys can apply encryption before transmitting files through Mover. Please note that if you encrypt files before transmitting them, some features may not be available.

Where Do I Report Security Concerns?

We take a number of measures to ensure that the data you transmit through Mover is safe and secure. While we're very confident in our technology, we recognize that no system can guarantee data security with 100% certainty. For that reason, we will continue to innovate to make sure that our security measures are state of the art, and we will investigate any and all reported security issues concerning Mover's services or software. For a direct line to our security experts, report security issues to legal@mover.io.

We will fully credit anybody whose reports lead to the improvement of Mover security.

Security in Depth

Summary

This whitepaper presents an overview of Mover's infrastructure with regards to security and how it fits into customers planned implementation. It will cover security policies and encryption.

Mover is a highly available infrastructure with the primary purpose of moving files between cloud storage providers. We provide a level of service tailored for the customer, and we understand that security and reliability are the most important features. We are dedicated to continually improving, and the policies presented here are to be considered the minimum standard of our implementation.

Security

Security for us comes in four primary areas:

1. Authorization of the service for a user.
2. Storage of user authorization information.
3. Protection of our infrastructure from external intrusion.
4. Security of a user's data as it flows through our system.

Authorization of service

During the process of authentication with a cloud storage provider or other service, we require the collection of authentication data to be retrieved and stored for later use. There are two primary methods that are used to collect this data, they are:

1. OAuth

OAuth (Open Authorization) is a web standard which provides a process for end-users to authorize third-party access to their server resources without sharing credentials. More information can be found at:

- http://en.wikipedia.org/wiki/OAuth
- http://oauth.net/

Although the exact encryption method varies browser by browser, Mover requires strong TLS encryption between Mover and the User for the initial authorization. All our OAuth token exchange use TLS v1.2 to connect to the authorizing server. OAuth will allow the user to deny Mover access to the third-party service at any time by revoking our token.

2. Direct password or key collection

All password or key collection occurs through the web interface over a secure TLS connection utilizing strong ciphers, generally 256-bit AES or stronger.

Storage of user authorization information

In order for us to have continual access to the user's service, we need to store authorization credentials. In the case of OAuth or OAuth like services, like Box, we store an authorization token which grants us access. In the case of a direct password or key, like FTP servers or Amazon S3, we need to store direct authorization credentials.

These credentials are the key to accessing the customer's files, and we take special care to secure this properly. All tokens and passwords are encrypted using AES 256 variant with both global and user specific encryption keys. This data is then stored in our internal database servers with no outside access.

Security of Infrastructure

It is important that our infrastructure is secured from external attacks. The following classes of servers have carefully implemented security policies:

1. Runners

Runners are our servers that move files. Since this entire process relies on outbound connections, our security policy can be very simple and secure. There is no outside access allowed to these servers. All outbound traffic is pushed through a point firewall, obfuscating the infrastructure behind.

For maintenance, SSH access is allowed through a two stage process. Access to the point firewall utilizing SSH keys only, then from there SSH access to the individual servers only via SSH keys. To further increase security, inbound SSH is only allowed from specific white-listed IP addresses.

2. API Servers

Our API servers, both for our public API and internal API, have a public facing interface. Similar to the Runners, the API servers have SSH management access through a two stage process. The main difference is that our API servers require a public facing web interface that is completely open. Only TLS web traffic is allowed into this interface. For our internal application API, only authenticated session based traffic is allowed. For our public API all access is secured through our managed API keys.

3. Web interface

All applications by Mover that have a web interface (ie. https://app.mover.io) are secured using TLS strong ciphers. User input, including username and passwords, are passed securely to the backend over this encrypted TLS connection, identified by our site-wide 2048-bit TLS certificate.

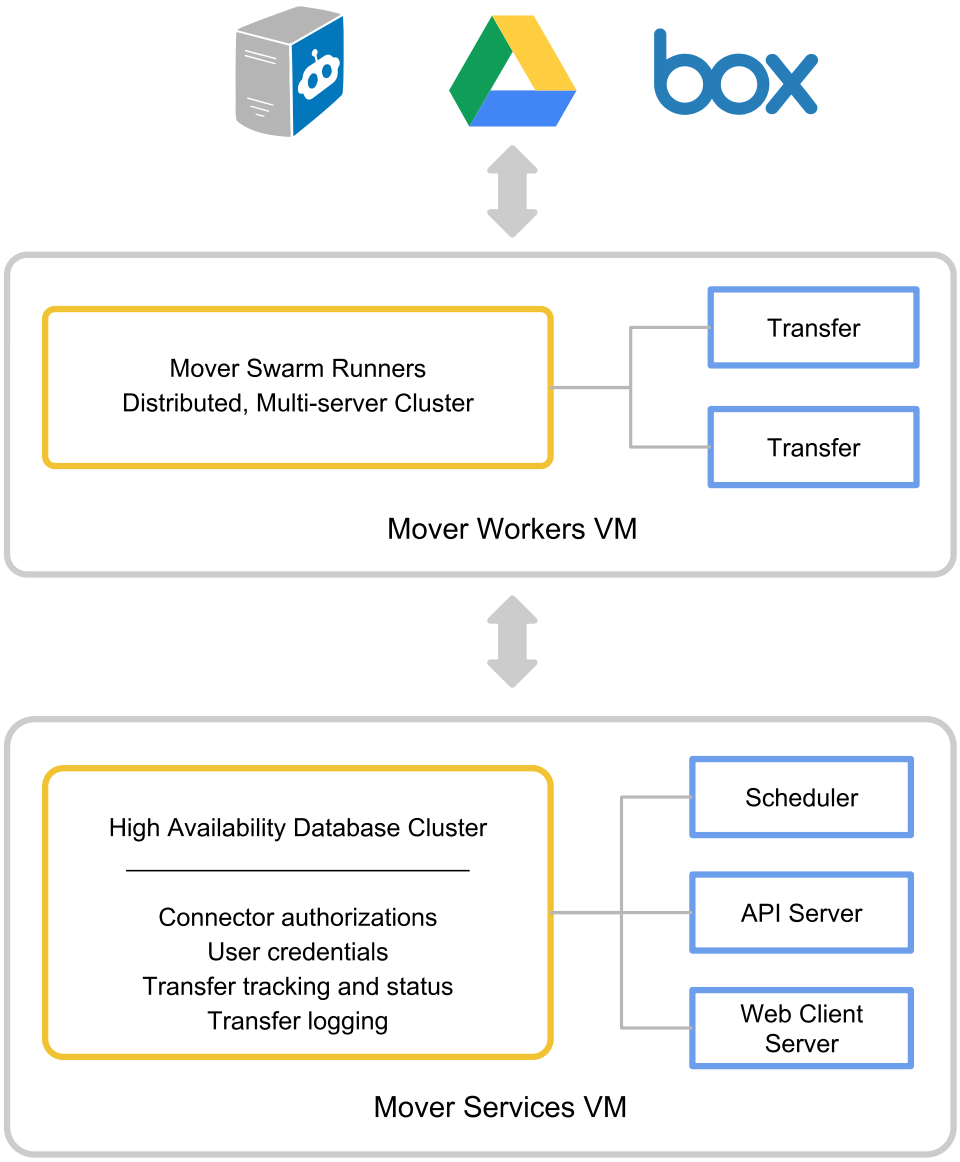
User data as it flows through us

During the process of a transfer, all files are downloaded to our Runner servers, then uploaded to the destination service. Each step relies on the security provided by the individual service that we are getting the files from, or uploading the files to. The following list describes the encryption available with each service:

No Encryption	TLS	SSH
• FTP • MySQL	• Amazon S3 • Box • Dropbox • Egnyte • FTPS • Google Drive • Office 365 • OneDrive • Rackspace • SharePoint • WebDAV	• SFTP

During mediation process, Mover maintains a copy of the file, temporarily, on an encrypted file system before it uploads it to the final destination. As soon as the file has been verified uploaded, we immediately remove the file from our cache. We never keep a copy of your data.

Architecture Overview Diagram


box
Mover Swarm Runners
Distributed, Multi-server Cluster
Transfer
Transfer
Mover Workers VM
High Availability Database Cluster
Connector authorizations
User credentials
Transfer tracking and status
Transfer logging
Scheduler
API Server
Web Client
Server
Mover Services VM