CloudFuze Security

Overview

The purpose of this white paper is to give you an idea of security measures taken by CloudFuze to protect the users' data.

Security

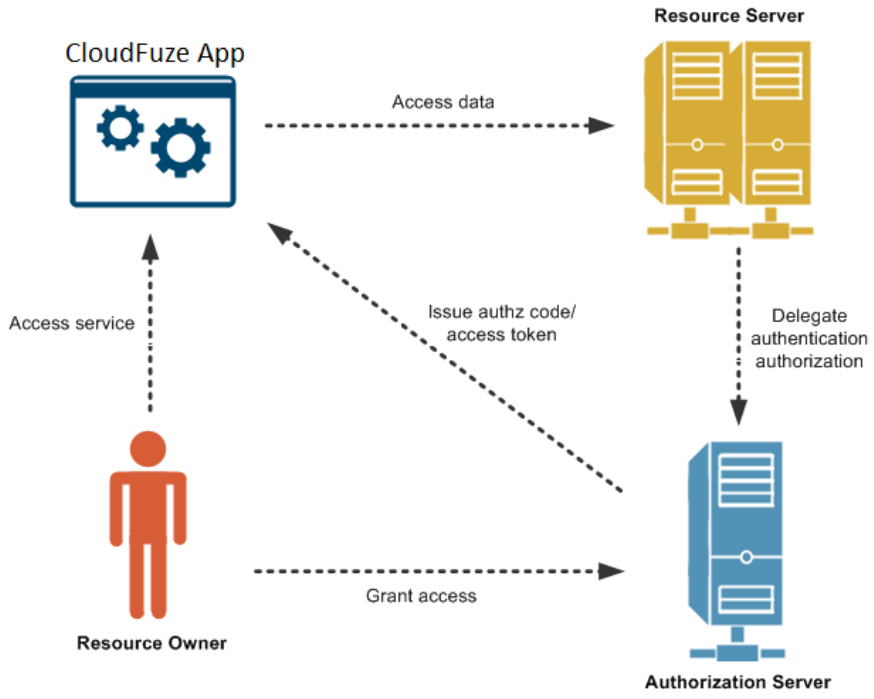
The following are the four primary focus areas for us when it comes to security.

1. Authorization of users' cloud service/services
2. Storage of users' cloud service authorization information
3. Security of users' data during the migration process
4. Defending our infrastructure from external threats

1) Cloud Service Authorization

To move data between cloud storage accounts and provide other CloudFuze services, we need to collect your authorization information and store it for future use. Depending upon on the type of cloud accounts/services, we follow two different methods to collect authorization information from you. One is OAuth protocol and the other is the direct password or key collection.

OAuth Protocol



OAuth is an industry-standard security protocol that cloud storage providers use to grant third-party services like CloudFuze a limited access to users' data and resources. OAuth eliminates the

need to share sensitive information like your cloud account passwords with CloudFuze. You can revoke access to CloudFuze from your cloud storage account at any time you want.

Direct Passwords and Keys

As not all cloud storage providers support OAuth, sometimes we require storing direct passwords or access keys. The collection of information like this occurs through CloudFuze's web interface over highly-secure TLS connection that uses strong ciphers, generally RSA-2048 bits.

2) Storage of Authorization Information

CloudFuze needs to store users' authorization information such as tokens, keys, and passwords to facilitate data transfers between cloud storage accounts/services. All of this sensitive data is encrypted using the RSA-2048 cryptographic cipher. We store this data in an encrypted form on our internal servers with zero access to outside parties.

3) Data Security During Migration

In most cases, CloudFuze uses data streams that are transferred from one cloud to another. Some cloud storage providers, OneDrive, for example, don't accept streams for large files that are greater than 100 MB. In such scenarios, we use file chunks (files in an encrypted and non-readable format) and send those individual binary chunks to OneDrive. We don't store users' data in any form.

4) Protecting Our Infrastructure from Intrusions and External Threats

Our data centers are SOC 1 and SOC 2 Certified. Here is a link to our data center provider's (CenturyLink) SOC certification information.

https://www.ctl.io/compliance/soc-2/

Our data centers are located in different places around the world where our instances are running. We have a manual DR policy which is to enable the paused cloud instance in a different region when there is a disaster in one region and update the DNS. We frequently test the DR switching policy. We tested the policy once in the last 90 days.

We use CenturyLink data centers for our IT operations. CenturyLink performs regular IT audits. The CenturyLink data centers are highly secured. The centers are certified even for government usage.

Online Resources:

CloudFuze Privacy Policy: https://www.cloudfuze.com/privacy-policy

CloudFuze Terms of Use: https://www.cloudfuze.com/terms-of-use

CloudFuze Report: https://www.ssllabs.com/ssltest/analyze.html?d=www.cloudfuze.com

OAuth related information: https://oauth.net

