Security Overview

Last updated Jun 6, 2020

This document describes security aspects of Afi Backup. The use of Afi services is governed by Terms of Service and Privacy Policy agreements. Afi works with leading cloud infrastructure providers to ensure the security and reliability of its service, in addition to:

- following a Secure Software Development Life Cycle (SSDLC);
- conducting regular vulnerability assessments;
- encrypting customer data in transit and at rest;
- adhering to other internal policies as described in this document.

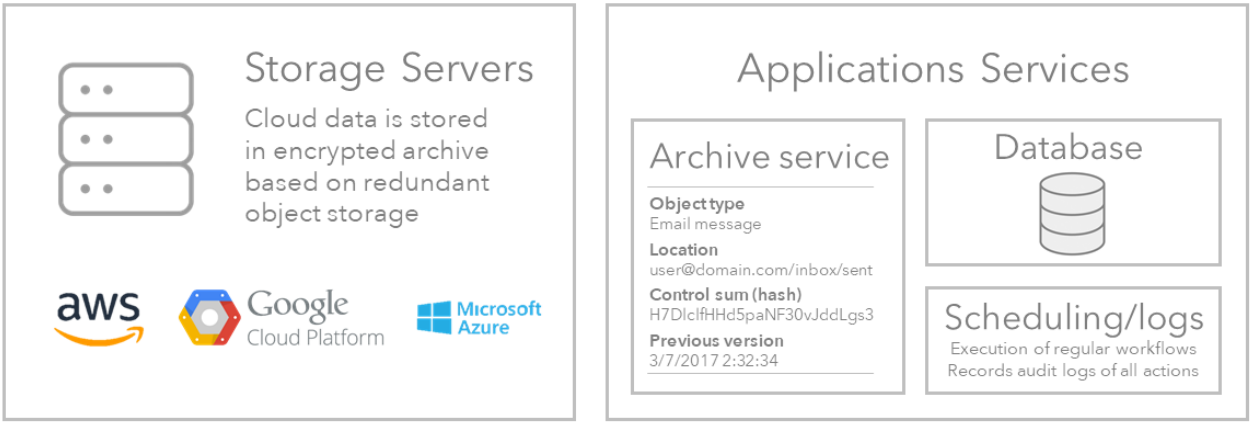
Secure Software Development Life Cycle

Afi source code is reviewed internally using guidelines from OpenSAMM and Microsoft SDL frameworks. Our software code is stored in BitBucket source code management system located in the United States. The system tracks source code access and modification activity.

The source code management system can be accessed only from devices that are compliant with Afi security policies. Only authorized R&D engineers access the source code and only for the tasks assigned to them.

Infrastructure

Afi relies on GCP, and/or AWS and Azure for cloud hosting and storage services. Customer data is stored in an encrypted archive (see "Encryption" section) on redundant object storage, and is accessed via Afi application services that manage user access rights and permissions.



Encryption

We use Transport Layer Security (TLS 1.2) cipher for data in transit. All data to and from our cloud service is encrypted using TLS 1.2. Data at rest is stored in cloud storage protected by Advanced Encryption Standard 256bit (AES256) cipher.

Compliance

HIPAA

We would like to emphasize, that there is no certification recognized by the US HHS for Health Insurance Portability and Accountability Act (HIPAA) compliance. Complying with HIPAA is based on vendor self-assessment.

Following HIPAA rules and provisions is a shared responsibility between Afi and Google. Afi application is compliant with HIPAA and we use GCP infrastructure that declares compliance with HIPAA. Business Associate Agreement (BAA) is available for signature per request.

Privacy Shield

Afi complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Afi has certified to the Department of Commerce that it adheres to the Privacy Shield Principles.

To access Afi Privacy Shield partner page, and to view our certification, please visit https://www.privacyshield.gov/participant?id=a2zt0000000PLVTAA4

Cloud Security Alliance Member

Afi is a member of the Cloud Security Alliance (CSA), an organization with a mission to promote the use of best practices for providing security assurance within Cloud, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.

PCI

Afi meets PCI DSS compliance requirements and shares this responsibility with GCP and Stripe. We use these infrastructure providers and they have been assessed by Qualified Security Assessors which validated specific requirements and found that they are compliant with PCI-DSS.

GDPR

The GDPR requires Afi to protect the privacy and personal data of EU citizens and transactions that occur within EU member states. All Afi products and services are compliant with the GDPR. Major GDPR requirements and Afi features that help to address them include:

- Storing and processing data within EU. Afi enables you customers to select where their data is stored by specifically setting the pre-defined destinations
- Right to erasure. Afi will locate and remove data from the system in a timely manner upon request.
- Security. All the customer data in transit and at rest is encrypted as described in "Encryption" section. Afi follows Secure Software Development Cycle as outlined in the respective section.
- Records of processing activities. Afi audit log provides visibility on all actions performed in the system and enables customers to retrieve these logs when required.

Other

Afi relies on Google Security Model that provides top-level security of the cloud to its customers which holds the following compliance certifications: SOC1, SOC2, SOC3, ISO 9001, ISO 27001, MPAA, FISMA, FERPA, CJIS, CSA, DIACAP, FedRAMP, ITAR, FIPS 140-2, G-Cloud.

Vulnerability assessments

Afi conducts application vulnerability testing internally on a regular basis. Our engineering team preforms regular security patches and upgrades. We share results of vulnerability assessments with the management and our board of directors.

Data Deletion Policy

In order to protects customers from data loss, Afi doesn't allow customers to delete or modify backed up data directly from Afi application. Customer data can be deleted from our servers after a request addressed to privacy@afi.ai by a domain administrator. Data from inactive non-paying customers is erased within 1 month of inactivity period/trial expiration. Send a request to privacy@afi.ai if you wish to erase the data sooner.

Credentials & Access Control

Afi does not require Google user credentials and we don't store your passwords on our servers. Afi cannot access passwords as we use OAuth 2.0 to access G Suite.

Our software is designed in a way to make it impossible for Afi employees to access encrypted customer data.

Disclosure Policy

We do not and will not provide any customer information to any organizations. Where required to do so by law, we will disclose customer information to law enforcement agencies in the United States and European Union. As of July 2019, we have not received any requests from law enforcement agencies and have not disclosed any customer information to them.