250 King St., #514
San Francisco, CA 94107
amadeus@mozartdata.com
http://www.mozartdata.com/

Mozart Data - Security Overview

Service Overview

Mozart Data is a web application that manages a Snowflake data warehouse (and associated compute resources and users), ETL pipelines, and the scheduling of SQL data transformations. Mozart Data also provides data analysis consulting.

Data Access & Control

Mozart Data uses role-based-access-control for all systems with access to each customer's data. Only one person at Mozart Data (CTO/co-founder) has access to each customer's Snowflake database. Within the Mozart Data web application, each customer can control role-based access (user/admin) to the site. By nature of the product, those roles have access to query the customer's Snowflake instance.

Non-sensitive data related to the customer (usage data, application events, etc.) are also protected by role-based-access-control, but are available to Mozart employees with a need to analyze user behavior or diagnose problems.

Mozart Employee Security

- Mozart Data's employees use Two-Factor Authentication for email accounts and many other services.
- Mozart Data performs background checks on all new employees.
- Mozart Data does not employ any offshore staff.

Authentication and Authorization

- Mozart Data stores secrets using Google Cloud Platform Secret Manager. That data is encrypted in transit with TLS and at rest with AES-256-bit encryption keys.
- Mozart Data uses token-based authentication for all API requests from the frontend to the backend servers, and uses Argon2 for password encryption. All authentication requests are rate-limited by IP.

Data Backups

- Mozart Data stores 7 days of backups of its web application data in its GCP Cloud SQL instance, which is encrypted and deleted after that retention period.
- Mozart Data uses Snowflake's standard "Time Travel" with 1-day retention and 7-day "Fail-safe" backups for each of its customer's data.

250 King St., #514
San Francisco, CA 94107
amadeus@mozartdata.com
http://www.mozartdata.com/

Data Displayed on Warehouse Clients

- The Mozart Data web app displays data on the user's screen and temporarily stores data in the browser to facilitate app functionality. All data on the user's browser is deleted when a user logs out.
- It is common for employees to connect your company's data warehouse to a business intelligence (BI) tool of their choice. BI tools may retain copies of your data so we recommend implementing an access control policy on your BI tool as well.
- If an admin revokes a user's access to the system, that user is automatically logged out of the Mozart Data web app, and all Mozart-related data stored on their browser is deleted. Any BI tool connected to Mozart Data with the user's login credentials loses access to the customer's data warehouse. Note that this BI tool might retain copies of data from before the user's access was revoked.

Data Logging, Monitoring, and Incident Detection

- Server logs are centrally stored in GCP "Operations Logging."
- Error logging and monitoring is handled by Sentry.
- Some application event logging is stored in Segment, and that data is replicated in Snowflake. No sensitive information is included in these event logs.
- Logs are retained for 3650 days (~10 years).
- Mozart Data uses the GCP Security Command Center for monitoring / alerting on potential security incidents.

Vendor Security Documentation

Mozart Data uses best-in-class security providers for a variety of services, including Google Cloud Platform (us-central region) for its web application hosting services, Fivetran for its data connector services, and Snowflake for its data warehouse services. As such, the security measures used by these providers also apply to each customer using Mozart Data. You can find links to each provider's security documentation below:

- Google Cloud Platform Security
- Fivetran Security
- Snowflake Security and Trust Center

Development Processes

- Production environments are entirely isolated from development and staging environments, and have no access to its data and secrets.
- Mozart Data uses protected branches and CircleCI for automated testing of all changes.
- Access to Mozart Data's repos are protected by multi-factor-auth, and all code changes are reviewed by at least 2 engineers. Access to Mozart Data's deployment server is also protected by 2FA, and only the protected master branch can be deployed. For more information, see GitHub Doc's section on protected branches.

250 King St., #514
San Francisco, CA 94107
amadeus@mozartdata.com
http://www.mozartdata.com/

End of Service

If a customer decides to stop using Mozart Data, or Mozart Data is unable to continue to provide its data services, all customer data in data warehouses will be deleted within 30 days following termination of the service. Server logs that include the customer's usage data and access will follow Mozart Data's 10-year log retention policy. Upon request, Mozart Data can work with the customer to export their data before the end of service.

Terms of Service and Privacy Policy

- Terms of Service
- Privacy Policy