CONSORTIUM

Metrics That Matter®

Security Protocols

At Consortium Networks, our client's safety and protection are paramount. We use rigorous security measures across all our products, from the testing phase to active use, to ensure your important information remains secure.

- Access to Metrics That Matter® (MTM®) is protected by a username and password of the user's choosing. A salted SHA512 hash of the password is stored in the database.
- User sign-ups are restricted to recognized email domains which are uniquely linked to company profiles. Unrecognized email domains are rejected without user knowledge.
- MTM® data is shared between user accounts of the same company.
- The data provided to MTM® is stored in a database on dedicated Virtual Machine hosts in Google Cloud. The VM disk is encrypted using AES-256 keys.
- All network traffic to the database is encrypted by TLS.
- Access to the database for manual maintenance is performed via a management console. Login to the management console requires SSO via Google Workspace which requires MFA.
- For efficiency, some data may be cached in an in-memory caching engine. Access to the cache is protected via authentication keys. All values stored in cache are encrypted with Fernet using a key that are known only to the API.
- User logins are managed via OAuth2 with access and refresh tokens stored in the user's local browser storage. Cookies are not used.
- Email addresses are verified on login every 60 days.
- We perform independent third-party penetration tests annually. The last test was performed in May 2022 by Neuvik.
- Attempts to login with an unknown username proceed with random fields based on a hash of the username. Only at the end of the login process is the user notified that the login attempt was unsuccessful.
- All changes to a user's authentication methods are sent to the user immediately upon change. Username and email cannot be changed by the user.
- Access tokens are valid for 20 minutes; refresh tokens are valid for 2 hours. Refresh tokens are updated on a rolling window: if a new access token is requested with a valid refresh token, the refresh token is extended to be valid two hours from the successful request. (i.e. The user is logged out automatically if he/she is inactive for 2 hours.)
- All tokens are signed by a 4096-bit RSA key and validated on every request.
- All tokens contain a unique key that corresponds to an entry in the database. The database entity is checked for validity for all requests. When a user logs out, that entry is removed from the database preventing the use of stale/cached tokens.
- The token database entry also contains a similar rolling expiration timestamp to the refresh token. In the unlikely event that a token would pass verification including the RSA key signing, there would still need to be a corresponding database entry for that token with a valid expiration timestamp.
- The API utilizes Google App Engine. The token signing key and the cache encryption key are injected into the API instances at launch and only exists in memory during runtime.

800-530-8350
contact@consortium.net
www.consortium.net

CONSORTIUM NETWORKS

2023-02-02