Consortium Networks

Metrics That Matter Security Protocols

CONSORTIUM
METRICS THAT MATTER

At Consortium Networks, our client's security is the foundation of our business. From our products in beta to live production, we employ strict security protocols to keep your critical data safe and secure.

The Details

- Access to the Consortium X 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.
- **Metrics That Matter** ("MTM") data is shared between user accounts of the same company.
- The data provided to **Consortium X** (including MTM) is stored in a relational database on dedicated Virtual Machine hosts in Google Cloud. The VM disk is encrypted using AES-256 keys.
- The database Virtual Machine hosts are only accessible via a private IP address in Consortium's Virtual Private Cloud. These hosts are not exposed directly to the Internet.
- All network traffic to the database is encrypted by TLS.
- Access to the database for manual maintenance is performed via a bastion host. Login to the bastion host requires an SSH encrypted session via the web console by a user with appropriate rights within Consortium's Google Cloud infrastructure. Direct SSH access to the bastion host requires a public SSH key stored in the user's Google Cloud profile.
- User logins are managed via OAuth2 with access and refresh tokens stored in the user's local browser storage.
- 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 is injected into the API instances at launch and only exists in memory during runtime.

Consortium Difference Makers

Email verification is required for new users via a one-time link sent to the email address the user provides.

Two-factor authentication is available via SMS configurable in the user profile.

Periodic security testing of the application is performed by a 3rd party. The most recent test was performed by Synack in October 2020.

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

CONSORTIUM
NETWORKS