Permissions, Privacy & Security
Platform Security

Information security is globally important and a topic of regular conversation. PubSafe, powered by Aftermath Data, wants users to be confident that industry-standard or higher, security practices are in place. Data is encrypted at rest (stored) and in transit (from the database to the mobile app or web portal) using encryption. Aftermath Data developers cannot view passwords or unique user information in the database which means if data was stolen, it would be almost impossible for anyone to unencrypt the data without government assistance. The simple reality is that the PubSafe data just isn't that important to cybercriminals. The low resale value means cybercriminals are more likely to focus on data from banks, small businesses, and other sources of credit and personal identity data which can be converted to cash by selling information on the dark web.

User information is never sold or shared with marketing companies. This prevents the data from being share unencrypted and potentially compromised by 3rd parties with less capable security. Unfortunately, no platform is hacker-proof as seen by the US government, along with major corporations like Colonial Pipeline, Microsoft Exchange, Apple, and others. Think about how many times you have to reboot your phone or computer to apply security updates. Most of the apps you use today are potential security leaks and likely do not maintain the backend security implemented by Aftermath Data for PubSafe. Aftermath Data relies on over 21 years of online security best practices to reduce the odds of a significant cyberattack.

The Aftermath Data infrastructure architecture is designed to provide multiple layers of protection. Security ranges from user settings to the technology used to build the mobile app and web portal, data sharing methods to the server configuration. It would not be wise to outline every security step taken which could aid potential cybercriminals.

General Security Implemented

- VPN connections
- Multiple layers of password-protected resources
- APIs
- 256-byte encryption
- Encryption at rest
- Encryption in transit
- Robust commercial-grade firewalls
- Data compartmentalization
- Complex and long passwords
- Employee cyber training
- Non-standard IP addresses
- Regular backups to other secure locations
- Tier 4 data centers or cloud services from platforms like AWS or Azure
- Regular and routine security patches to servers and to mobile devices, and workstations using Microsoft 365

Permissions, Privacy & Security

Unique solution ID: #1077
Author: Aftermath Data
Last update: 2021-09-27 17:53