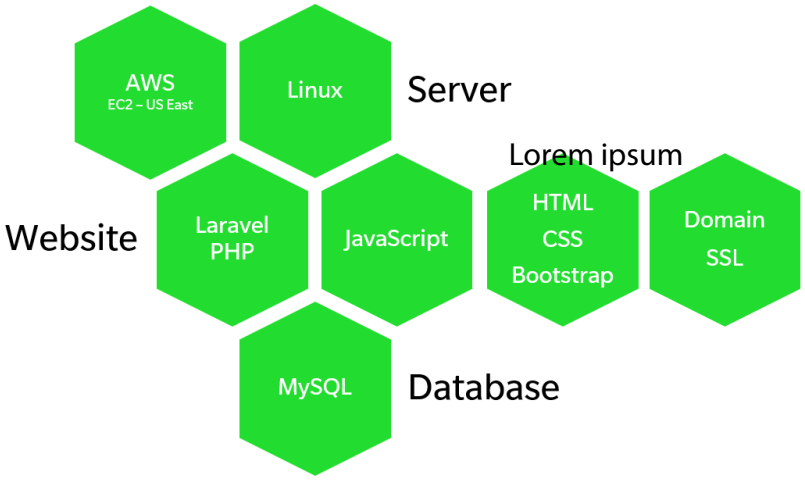
Technical Security Information

TeamTexter® v 2.0 - Web Application

At A Glance

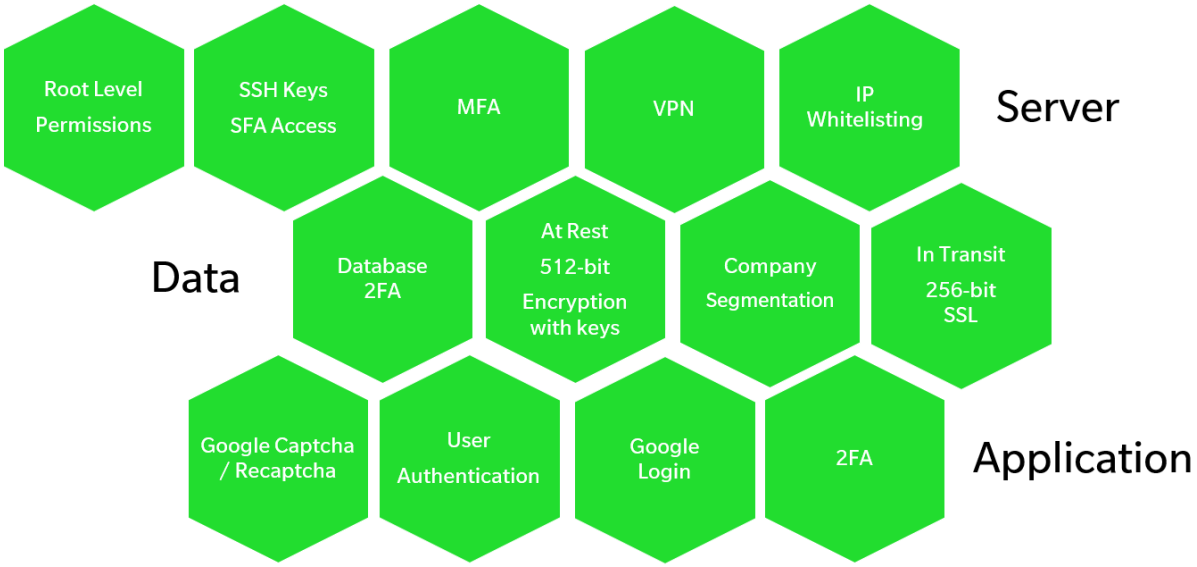
Tech Stack

We use Amazon Web Services to host and secure the TeamTexter v2.0 Web Application. The TeamTexter v2.0 service is alone in it's Amazon account with no other shared services. We maintain two separate servers; one for testing/dev and one for production.



Security

We give great care to security and employ a number of tools to ensure data is secure at rest and in transit.



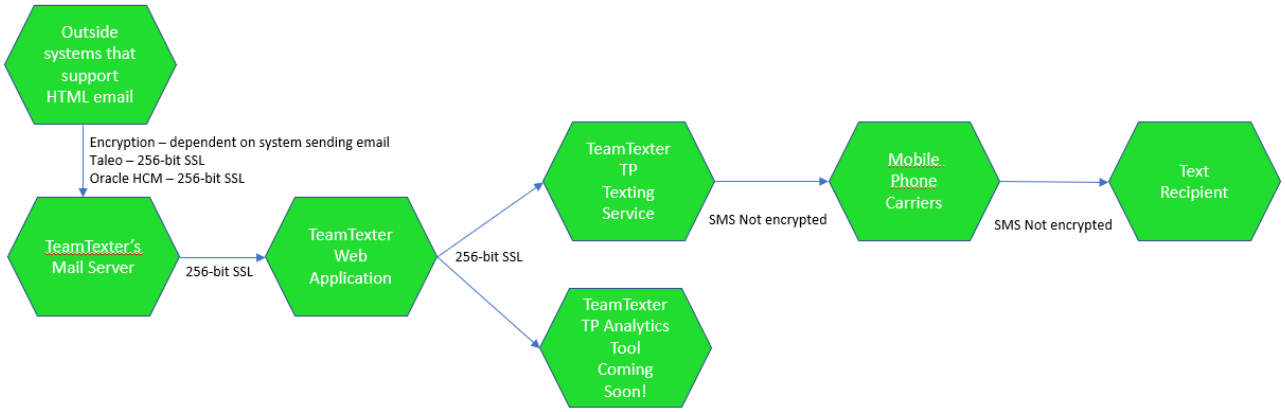
Technical Security Information

TeamTexter® v 2.0 - Web Application

At A Glance

High Level Application Interfaces

Our application uses a number of APIs to gather and deliver data to and from services that are used for texting, emailing and reporting. This is a very high level diagram showing the connections.



Your Data

TeamTexter v2.0 stores personal infromation such as user email addresses, mobile numbers and names. It also stores data about the recipients you are texting such as name and mobile number. Teamtexter v2.0 stores your text message content. Web browser cookies and cache are utilized to store data within the web application.

Web Browser Data: IP Address, Device Type, Geolocation, Cookies, Web Tokens

User Information: Name, Email Address, Mobile Number, User Name, Password.

Text Recipient: Name, Mobile Number, Opt In Status, Opt Out Status.

Text Message Content: Date, Sent To, Sent From, Message Content

Technical Security Information

TeamTexter® v 2.0 - Web Application

More Details

Application User Authentication

Users create an account through application at app.teamtexter.io by providing their name, email address, password and a unique company code. Sub-users are invited to join the account when an account owner creates a subuser account for them in the application. Sub-users are invited to join by email. All users will assign their own password and use the unique company code to login. Forgotten passwords can be reset by clicking the forgot password link.

Data Storage At Rest

Data sent to TeamTexter through outside systems and users will be kept inside the source system by its native functionality. Data is stored within the MySQL database on the AWS server and is 512-bit encrypted. Your data is always stored within the United States. Our servers are secured by a number of measures such as VPN, IP whitelisting, MFA, root-level permissions and a firewall. Data is backed up daily.

Data In Transit

As requested by a user of TeamTexter, data is sent to TeamTexter's third party texting service to ultimately be delivered to a text recipient. During the transit to the texting service, the data is secured by 256-bit SSL through a proprietary API. Data sent from TeamTexter's mail server to the TeamTexter application is also secured by a 256-bit SSL connection. Any and all connections into and out of TeamTexter's service are secured by a 256-bit SSL connection.

Domain Security

TeamTexter uses many domains and subdomains, all of which have decurity certificated installed and verified from a Tier A trusted security company. User name, password and 2FA are used to validae any domain level changes.

Internal Controls

Network Security is maintained and verified by a third party IT infrastructure team who periodically run stress tests to diagnose and secure potential vulnerabilities. We protect our code development. In addition to undergoing a 3rd party code review for any regularities, our multi-layered authentication is able to block unauthorized access. All developers undergo an extensive vetting and hiring process. We update and store code regularly in GitHub. Lastly, Paramount Technology Solutions, LLC, TeamTexter's parent company, is currently undergoing exercises to prepare for its very first SOC 2 audit. We will be happy to share results when available.