StormAI

Stormboard

Security Overview

Stormboard's Data-First Platform prioritizes privacy and security by adhering to industry-standard security protocols and best practices to safeguard the confidentiality and integrity of user data. We send encrypted Storm data to our AI Service partners, including Microsoft OpenAI Service. Unlike ChatGPT where your chats can be used to train their model, Stormboard data is not used by our AI Service Partners to train their models. Data may be retained for up to 30 days in a dedicated single instance and accessible only to authorized employees for (1) debugging purposes and (2) investigating patterns of misuse. You can configure what data (Personal Identifiable Information [PII]) from your Storm gets redacted before sending it to our AI Service partners.

StormAI Security and Data Protection

StormAI prioritizes privacy and security, ensuring that user data and information are protected. It adheres to industry-standard security protocols and best practices to safeguard the confidentiality and integrity of user data.

Data Usage

As one of the initial AI service partners, StormAI uses the Microsoft Azure OpenAI API to transmit contextual prompts, as well as appropriate information and related Storm metadata to the Azure OpenAI engine.

Data Storage, Transfer, & Encryption

Stormboard and StormAI never use customer data to train the AI engine and all data is encrypted (both at-rest and in-transit). Data may be retained for up to 30 days in a dedicated single instance and accessible only to authorized employees for (1) debugging purposes and (2) investigating patterns of misuse. All data transfer to and from our Cloud services is encrypted with Transport Layer Security (TLS). Stormboard's implementation of TLS uses strong ciphers and protocols by default.

Microsoft Azure OpenAI Service

With Azure OpenAI, customers data is protected by the trusted security capabilities of Microsoft Azure while running the same models as OpenAI.

StormAI Administrative Controls

StormAI is an optional service for Stormboard customers. It is not a standard feature, and therefore can be disabled at an account level at any time. StormAI has no impact on the standard security model of Stormboard; when StormAI is not in active use, all data by default is protected by the Stormboard security and privacy protocols established for all customers and has no connection to the Microsoft Azure OpenAI service.

Note: Only a ***Storm Administrator*** can leverage StormAI (only licensed Members on your Team can become Storm Administrators – Guests cannot).

Note: StormAI can be set to disabled by default at a Team level – and can be enabled on an individual Storm-by-Storm basis.