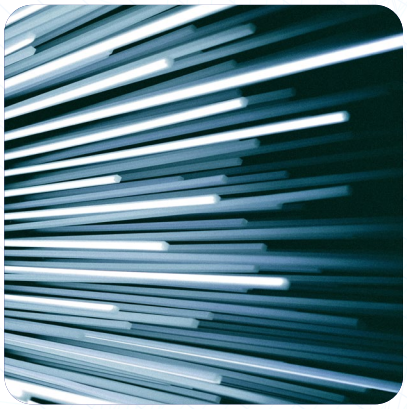
BriefCatch

BriefCatch Security

Summary

BriefCatch implements a comprehensive security framework designed specifically for handling sensitive legal documents in law firms, courts, and government agencies. The platform operates as a Microsoft Word and Outlook Add-in that processes text entirely in volatile memory (RAM), ensuring that no document data is ever stored or retained on disk. All data transmission occurs through HTTPS with TLS encryption, maintaining security during transit between the user's environment and BriefCatch servers.



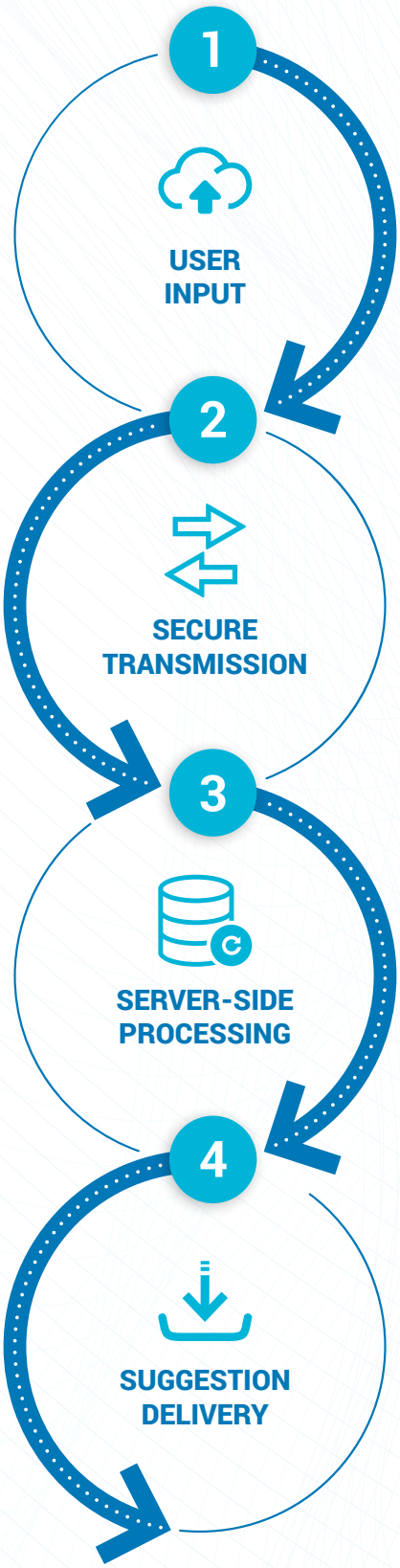
BriefCatch Data Security

Developed under BriefCatch's rigorous security standards, built for the Am Law 200.

At BriefCatch, we understand the critical importance of safeguarding sensitive information, especially for leading law firms that handle confidential client data. This document outlines how data flows through our system, providing transparency into our processes and demonstrating our strict adherence to privacy and security best practices.

Key Assurance

Document data is *never stored or retained* at any point in the workflow.



1. User Input

BriefCatch operates as a Microsoft Word and Outlook Add-in, allowing users to interact with the application directly within these programs. Users don't input document data into BriefCatch—instead, they activate the application, which analyzes their text and provides suggestions.

2. Secure Transmission

Once the user submits their document for processing, the text is securely transmitted over the network using **HTTPS with TLS encryption**. During this phase, the data exists in volatile network buffers and is cleared immediately after the data transmission is complete.

3. Server-Side Processing

At the server's API endpoint, the text is temporarily loaded into memory for processing. This processing involves several discrete steps:

- **Paragraph Tokenization**: The text is split into paragraphs within memory.
- **Tokenization**: Paragraphs are further broken down into individual words and punctuation (tokens).
- **Part-of-Speech Tagging**: Each token is analyzed to determine its grammatical role (e.g., noun, verb).
- **Grammar and Style Checking**: The tokens are validated against grammar and style rules to identify improvements.
- **Spell Checking**: The tokens are checked against a dictionary to identify spelling errors.

Each step occurs sequentially in **volatile memory (RAM)**, and the data is cleared immediately after the corresponding processing stage is completed.

4. Suggestion Delivery

Finally, the processed results are securely transmitted back to the user's browser over HTTPS. Network buffers are cleared immediately after this transmission.

Throughout this process, *user text* is never stored on disk. All operations occur in volatile memory and are cleared promptly to ensure maximum security and privacy.

Key Security Features

End-to-End Data Encryption

All document data is transmitted over a secure, encrypted channel using **HTTPS with TLS encryption**. This ensures that any data sent between the user's browser and BriefCatch servers remains protected.

No Data Retention

User text data is processed in **volatile memory (RAM)** and is cleared **immediately** after processing. At no point is user text stored on disk or retained by our servers. **Error metadata**, which may include non-identifiable technical details (e.g., rule positions), is logged **temporarily** and cleared on a regular schedule.

Minimal Data Exposure

Data processing occurs in memory for short durations, and each step of the process clears the data before proceeding to the next.

No User Text Logging

We do not log user text, ensuring that sensitive document content is never written to server logs or stored anywhere outside the user's environment.

Frequently Asked Questions

1. **Is my firm's data stored on your servers?**
   No. Document data is only processed in temporary memory (RAM) and is cleared immediately after processing. Nothing is stored on disk.

2. **How is data transmitted to and from BriefCatch?**
   Data is transmitted over an encrypted network using **HTTPS with TLS encryption**, ensuring confidentiality and security in transit.

3. **What data, if any, is logged?**
   Only **error metadata** (e.g., rule positions, technical diagnostics) may be logged temporarily for troubleshooting purposes. No user text is included in these logs, and metadata is cleared on a scheduled basis.

BriefCatch: Document Data Journey

Document data is never stored or retained!

STEP	LOCATION	DATA SET	MEMORY TYPE	MEMORY CLEARED?	STORED ON DISK
Input Reception	User's Browser or Office Sidebar	Text input entered by the user	Volatile (Network buffers)	Yes, when browser tab or session ends	No
HTTP API Request	Network (Transmission)	Text sent over HTTPS, TLS encrypted	Volatile (Network buffers)	Yes, cleared after data is sent and received	No
Input Text Processing	Server (API endpoint)	Received text temporarily in memory for processing	Volatile (RAM)	Yes, cleared immediately after processing	No
Paragraph Tokenization	Server (API endpoint)	Text split into paragraphs in memory	Volatile (RAM)	Yes, cleared after tokenization	No
Tokenization	Server (API endpoint)	Paragraph text split into tokens (words/ punctuation)	Volatile (RAM)	Yes, cleared after tokenization	No
Part-of-Speech Tagging	Server (API endpoint)	Tokens analyzed for grammatical roles	Volatile (RAM)	Yes, cleared after tagging	No
Grammar and Style Checking	Server (API endpoint)	Tokens checked against rules in memory	Volatile (RAM)	Yes, cleared after checks	No
Spell Checking	Server (API endpoint)	Tokens validated against a dictionary	Volatile (RAM)	Yes, cleared after spell check	No
Error Metadata Compilation	Server (API endpoint)	Error metadata (e.g., positions, rules)	Volatile (RAM)	Yes, after generating structured outputs	No
HTTPS API Response	Encrypted network (Transmission)	Response sent to client (browser or app)	Volatile (Network buffers)	Yes, cleared after transmission	No
Error Metadata Logging	Server logs (not including any document data or metadata)	Error metadata only (if logged)	Non-Volatile (Disk)	Yes, when cleared on default schedule for GCP	Temporarily
User Text Logging	N/A	No user text logged	N/A	N/A	No