casetext

Casetext and Cocounsel

Security Overview

2023

Contents

Casetext security policies

Data security is embedded into all our processes, which we continually improve. We ensure all your information—and your clients'—is always protected.

Casetext's trusted security program includes the governance and technical controls to ensure the platform, data, and code are secure and monitored.

- Our security policies align to NIST 800-53 Moderate and NIST Cybersecurity Framework (CSF), the basis of our comprehensive security program.
- We maintain a mapping of our controls onto ISO 27001 and SOC 2 standards.
- Casetext is on track to obtain SOC 2 attestation in 2023.

Trusted by the Am Law 200

And relied on by 10,000+ firms

More than 40 of the firms in the Am Law 200 have subjected Casetext to rigorous security review. Thousands of client firms, from solo and small practices and those in the Am Law 200, to in-house legal departments and legal aid organizations, trust Casetext to securely manage their most sensitive data.

> Casetext has transformed the AI landscape with CoCounsel. The power of this technology, deployed in a product that is secure and reliable, is a huge leap forward in what legal technology can do.
>
> **Scott Bailey**
> Director of Research & Knowledge Services, Eversheds Sutherland

Data encryption practices

All data are encrypted in transit and at rest in Casetext's systems.

We also require our sub-processors to encrypt all in-transit and at-rest data. And secrets are encrypted using Google Manager Keys backed by Google's Key Management Service.

Data in transit

Casetext secures all data in transit via TLS 1.2+. We only share data with vendors that demonstrate they have policies and procedures in place to protect the shared data.

Systems configuration

Systems are configured to require the TLS protocol, meeting industry standards for externally facing systems.

Data at rest

Symmetric encryption (AES-256) is used to protect data at rest. This ensures data is only viewable by authorized users.

Configuration assessments

Up-to-date assessments of our TLS configurations are available from Qualys's SSL Labs, by visiting SSL Labs SSL Test.

54%

of organizations use encryption to protect sensitive data in the cloud.*

58%

of IT professionals consider encryption the most effective way to secure data.**

86%

of organizations use Advanced Encryption Standard (AES) encryption algorithm.**

* Thales Group
** Ponemon Institute

Independent verification and auditing

Casetext has partnered with sophisticated external security resources to ensure we properly execute our security program.

We treat consistent monitoring of our platform through regular vulnerability assessments and penetration tests, along with review of our policies, vendor management, and risk management programs, as critical for our information security program.

Casetext relies on our relationships with security, compliance, and governance partners to ensure our company security program is held to the highest standards.

Stringent vendor management

Any major project budget specifically includes a line item for security

We have implemented a vendor management program requiring that each provider be tracked, approved for access, and reviewed quarterly. This applies both to vendors or contractors that assist with internal company operations and to vendors that supply SaaS or other solutions Casetext chooses to leverage. Casetext re-evaluates vendors when contracts or service delivery changes. We explicitly track vendor security incidents and ask all vendors to provide evidence of their security program and the security of their vendors.

Although cybersecurity is a never-ending task, Casetext has consistently demonstrated its commitment to it and has the appropriate policies, plans and resources in place to deliver a trustworthy solution.

Matt Konda
CEO, Jemurai

Casetext application security

Security is the cornerstone of all our applications, and we prioritize leading among our industry peers.

- All user access is protected by industry standard, role-based authentication.
- All access to data sources, queries, and results is logged and audited.
- Single Sign On (SSO) is available and integrates with your secure identity provider.
- Perimeter firewalls block unauthorized ports and protocols.
- All code is thoroughly reviewed and tested before deployment to production.
- Data source credentials are encrypted and stored in a secure secrets manager.
- Customer instances and data are logically separated.
- All data is encrypted in transit and at rest.
- Network vulnerability scans are performed monthly.
- Third-party penetration testing is performed annually.

Additional security programs

We annually review and test our Incident Response and Business Continuity/Disaster Recovery Plans and closely manage hardware, software, and access.

Annual security training

We require annual security training for all Casetext employees, including review of and attestation to Casetext's Information Security & Privacy Policies. Our annual secure developer training is based on OWASP Top 10.

Asset inventory tracking

Our asset management policies require tracking and inventory of all assets. Antivirus and mobile device management is installed on all laptops. Auto-updates and hard drive encryption are enforced.

Fully monitored access

Our identity and access management program ensures data is only available to appropriate parties. Casetext employees are granted platform access for administration purposes only, and such access is fully monitored and regularly audited.

Robust vendor vetting

We maintain a robust vendor management program and require vetting of all third-party software and contractors. We explicitly capture, track, and approve all vendor access to Casetext data and review and approve all connections that share data with vendors.

Reliable AI legal assistance

CoCounsel lets lawyers delegate a broad range of substantive legal work to AI.

CoCounsel is a software application launched in March 2023, built by Casetext and customized for legal practice, and powered by GPT-4, the most advanced large language model from OpenAI. Lawyers can trust to CoCounsel work they might previously have delegated to a paralegal.

CoCounsel capabilities

CoCounsel reads, analyzes, and summarizes documents. Users delegate tasks including document review, deposition prep, legal research memos, and contract analysis to CoCounsel through a single interface.

User-controlled data

CoCounsel customers retain all rights to their data. Data they enter into the application is only used by Casetext to serve the product to users and can be deleted by users at any time.

User data privacy

Data entered into CoCounsel is never used to train the AI model, which is accessed via dedicated, private servers. Data is encrypted in transit and at rest in Casetext's GCP environment, and never stored by our AI partner.

CoCounsel uses our proprietary search technology to surface more accurate, on-point information than possible by directly accessing general-purpose large language models (LLMs).

Unlike even the most advanced LLMs, CoCounsel does not "hallucinate." By limiting the model to known, reliable data sources, such as our database of primary law, updated daily, we enable accurate results, every time.

CoCounsel makes it easy for users to validate output. Answers link to their origin in the source materials so lawyers can confirm every answer themselves, just as they do with human-generated work.

Our Trust Team—AI engineers and attorneys—ensures quality and accuracy across the platform. Before launch, they spent 4,000+ hours fine-tuning CoCounsel's results on 30,000+ legal questions.

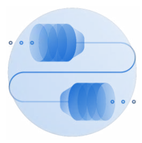
Before launch, CoCounsel was used 50,000+ times in real-life legal work by our team of beta testers: 400+ lawyers from elite law firms, boutiques, in-house, and nonprofits.

How we serve the CoCounsel application

CoCounsel is a cloud-based application, and all data is stored in Casetext's Google Cloud environment.

Dedicated instance of GPT-4

GPT-4, the most advanced LLM from OpenAI, provides CoCounsel's advanced language capabilities. CoCounsel accesses the model through a private server, and no user data or documents entered into CoCounsel are ever retained by OpenAI or used to train GPT-4 or any AI model.



No AI partner data storage

Any user information required to perform a task in CoCounsel is sent to OpenAI's Microsoft Azure, US-based servers only for the time it takes to process the request. OpenAI is contractually prohibited from storing user data beyond processing. The life cycle of the data is equal to the https request, and there is no data written to disk.

Limited data retention

Casetext retains search history, metadata, prompts, and completions only for the purpose of providing the CoCounsel application to users and for no other purpose. Data is stored and encrypted at rest with AES-256 in Casetext's GCP US-West environment. Users may delete their content in the application at any time.

GCP and AWS cloud services

All data stores and services are hosted in US-West regions of the Google Cloud environment. The user-facing CoCounsel web application is served from a Heroku (AWS) Private Space in the US-West region.

The secure way to use AI in legal practice

Chief among lawyers' obligations is to protect the confidentiality of privilege, work product, and client data.

All user data entered into CoCounsel is subject to rigorous security controls. These safeguards are in stark contrast to how data is handled by consumer-facing LLM-powered products such as ChatGPT or GPT-4, which lack the security and privacy guarantees client work requires.

Private, dedicated servers

CoCounsel accesses the underlying AI model through private, dedicated, Microsoft Azure US-based servers and through a zero-retention API that entitles Casetext customers to the most advanced data security controls available.

Customer data

No prompts, results, or any customer data whatsoever (including any auxiliary information related to those search queries) entered into CoCounsel that are processed by the AI model (GPT-4) are used to train the underlying model.

User-controlled data

Users retain ownership of, rights to, and control over their data and can remove it completely from the CoCounsel platform at any time. Customers also fully own their query response data, which can be deleted upon request.

Strict data retention limits

OpenAI is contractually prevented from storing any customer data longer than needed to process requests. The life cycle of the data is equal to the https request, and there is no data written to disk.

> CoCounsel provides efficiency gains that are applicable in several of our practice areas. The tool allows our attorneys to explore new options to meet our clients' needs while providing the security and guardrails they expect.
>
> **Myka Hopgood**
> Senior Director, Strategic Legal Innovation, Dykema

casetext

casetext.com
security@casetext.com