Secure AI

Redwoods Research

Secure AI is the world's first and only end-to-end encrypted AI Large Language Model (LLM) inference. It runs public, open weight, read-only LLM models; like Qwen, Mistral, and GPT-OSS. These models run inside a trusted execution environment secured to each user via public key cryptography. We have a prototype available for customer demonstrations as well as operational instances deployed in air-gapped environments.

Secure AI can be built to spec, tailored to immediate needs, deployed quickly, hosted in your environment or our secure data center. From the field to headquarters, only the user account holds the private key. We store the encrypted chats and public key in our database. The user solely controls the access to the encrypted data with the ability to export the queries or results as they desire. All data is encrypted and zero logs are kept or retained about usage. The user can export their queries but otherwise everything is end-to-end encrypted. No one can steal, see, modify, lose, nor sell any of your queries, conversations, database of users, or other data. It is blind, even to us.

Why Secure AI?

Beyond being the only end-to-end encrypted AI, each instance is built to customer requirements, customized as desired. We can provide rapid deployment at the location, price point, and service model the mission dictates. Customers may buy the box and have us build on site, ship a finished product, have us host customer owned in a secure datacenter, or subscribe to Secure AI hosted on our hardware. We sell GOGO[1], GOCO[2], or COCO[3].

We run everything in a Trusted Execution Environment (TEE) for encrypted computing to occur outside the normal operating system. This allows the user queries and data to be: encrypted at rest with the public key cryptography; encrypted in transit with the public key cryptography; and encrypted processing within the CPU itself, outside of the operating system. This setup provides end-to-end security and privacy of data exchanged with the AI models. Your data is yours. It is impossible for us or anyone else to see or use your data. Your queries are not used to train our model. We train your specific instance on the data sources your mission requires, be they OSINT, private data, or a mix of both.

Redwoods Research fully supports customers wishing to sustain the tools they purchase from us. We offer training to your technical support team and users. While competitors may insist on maintaining their propriety systems, we believe you own what you buy.

Alternatively, we can offer fast, responsive, human support direct from the developer via end-to-end encrypted chat, voice, or teleconference for screensharing. Security comes with constraints; we cannot reset passwords nor rescue lost passphrases (their private key), should the user lose access or forget. On account signup, we use a wizard to walk the user through creating their passphrase/private key and a recovery phrase to regenerate their private key in the future. The wizard requires the user enter 5 random words from the recovery phrase to confirm they have it stored somewhere on their system or person.

1 Government Owned, Government Operated
2 Government Operated, Contractor Owned
3 Contractor Owned, Contractor Operated

CONTACT US

www.redwoodsresearch.com sales@redwoodsresearch.com

#DUNS Number 11-933-9939 SAM.gov Unique Entity ID: RSCXUUNXND28 SAM.gov CAGE/NCAGE: 0YGF1 #CAL E-Procure Bidder/Supplier ID: BID0118873