

The Global Relay security combination

Global Relay integrates security in every aspect of our services to keep your records secure, available, and tamper-proof

Key security differentiators

Hardware security modules

Sophisticated physical devices store private encryption keys and ensure that they are never seen by human eyes. This means that offsite decryption of customer data is almost impossible without access to our key management services.

Reconciliation

A thorough process occurring during receipt, archiving and deletion ensures that every message is accounted for and has a full audit trail.

Audits and certifications

We are ISO 27001 certified, and our primary and secondary data centers are SOC 2. We also operate within the NIST and CIS security frameworks.

Efficient due diligence

We complete hundreds of due diligence exercises per year for existing and prospective customers. We will work with you to complete your due diligence efficiently, providing accurate and complete information until you are satisfied that our security systems meet or exceed your expectations.

Constant integrity checks

We ensure that messages are not removed, tampered with, or otherwise altered over the entire lifetime of the messages by comparing the hashes of the encrypted messages with the hashes of the messages when they were ingested. Checking runs continuously from the point we receive a message until it is permanently deleted.

Monitoring and logging

A dedicated 24 x 7 global security team continuously monitors all systems, logs, and threats. In addition, detailed logging for each customer tracks every file operation and user action. This data is made available via an Event Log API to feed your own security and event information management (SIEM) tool.

Private ownership

We are privately owned which allows us to make long term investment decisions to design and build lasting and resilient services. For example, we have built and continue to manage our own private primary data center, and we continue to invest heavily in state-of-the-art security and AI hardware.

Responsible approach to AI

We host our own AI infrastructure and never train models with your data without written consent. We are committed to ensuring our AI usage is transparent, explainable, and aligned with our values and security principles.