

GLOBAL RELAY: SAFEGUARDING THE SECURITY OF eCOMMS & TRADE DATA

Since its founding in 1999, Global Relay has never experienced a single security or privacy breach – and has continued to maintain an excellent uptime record.

To protect the security, integrity, and availability of data in its custody, Global Relay implements various policies and processes, which include:

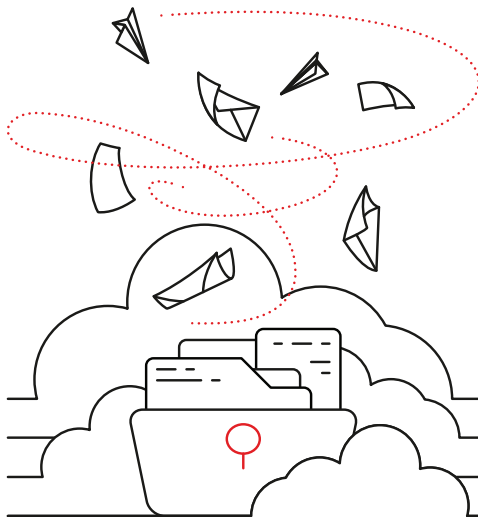


ESTABLISHING A SINGLE SOURCE OF TRUTH

Global Relay Archive natively captures and stores all data in a secure, unified, and tamperproof cloud repository.

It preserves a ‘gold copy’ of every business and trade communication – an indisputable record of ‘who said what, when, to whom’ – that will withstand court and regulatory scrutiny.

As an organization’s system of record – the single source of truth for all its business and trade communications – Global Relay Archive ensures a clean chain of custody, and consistent search results, which are critical during audits and investigations.



PRESERVING DATA ACCORDING TO COMPLIANCE RULES

Global Relay Archive preserves complete, accurate copies of eComms and trade data according to U.S. SEC Rules 17a-3 and 17a-4, FINRA Rule 4511, and other compliance recordkeeping regulations.

As such, Global Relay Archive:

- Only imports data that meets quality standards
- Preserves tamperproof copies of every archived communication
- Verifies the quality and accuracy of the storage media recording process
- Replicates data to its secondary data center in near-real time
- Logs all actions on archived communications in unalterable audit trails
- Stores archived data and indexes on RAID 6 devices, with checksum error correction



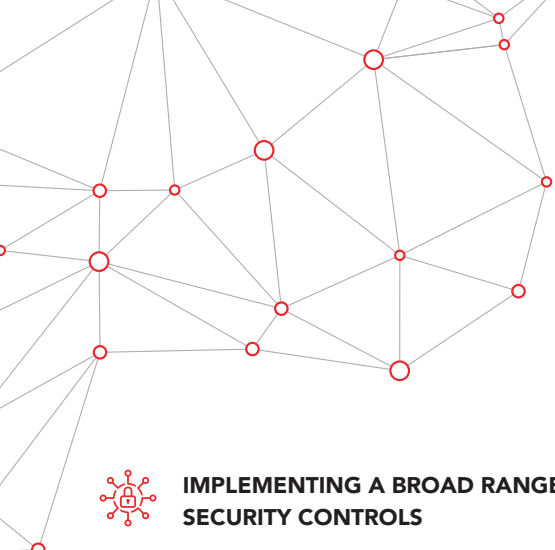
RETAINING FULL AUDIT TRAILS ON ARCHIVED DATA

Role-Based Access Controls (RBAC) determine the access rights of users within an organization to their archived data, and to data review and supervision tools available to them.

Global Relay Archive logs all user actions on archived data in an unalterable audit trail, documenting:

- Who ran the search, viewed the data – and when
- What action was performed – for example, set retention term
- Any comments/notes provided

Audit trails are retained for the life of the archived message, and can be searched and viewed by authorized users.



CONTACT

Visit: globalrelay.com
Call: North America: 866 484 6630
 Europe: +44 (0) 203 206 1850
Email: info@globalrelay.net



IMPLEMENTING A BROAD RANGE OF SECURITY CONTROLS

Global Relay implements a host of security controls, namely:

- **Physical**, which include restricted access to data center (DC) and office facilities; 24x7x365 security, surveillance and monitoring; and a dedicated server room (primary DC) and cage (secondary DC)
- **Environmental**, such as HVAC systems, fire detection/suppression systems, UPS, and backup generators
- **Technical**, such as firewalls with malware and IPS inspection, a DMZ, network and host-based IDS/IPS, in-transit and at-rest data encryption, vulnerability scans, pre-release application testing, and data replication to secondary data center
- **Organizational**, which include comprehensive employee criminality and identity checks, and restricted and monitored employee access to archived data using Role-Based Access Controls (RBAC)



HOSTING DATA IN A DATA-SAFE LOCATION

Global Relay's data centers are located in Canada, recognized as a 'data-safe zone' by the EU, United States, Asia, and much of South America due to its stringent privacy and data protection laws.

Global Relay is subject to PIPEDA, Canada's federal data protection law. The European Commission has twice audited PIPEDA, and determined that it provides protection equivalent to or better than the GDPR.

This means EU firms can use Global Relay services without needing additional safeguards to meet the requirements of the EU Data Protection Directive or the GDPR.



MAINTAINING FULLY REDUNDANT SYSTEMS

Global Relay's cloud service is hosted in two mirrored, geographically dispersed data centers. The systems within each data center are fully redundant. If the primary data center is lost, services fail over to the secondary one.

Global Relay Archive preserves four copies of every message – that is, two in every data center. Archived data is replicated in near-real time to the secondary data center, which functions as a data recovery site.

Global Relay data centers are more than 2,500 miles, or 4,000 kilometers, apart. Geographical diversification reduces the risk of losing both data centers should a natural disaster or other catastrophic event occur.

