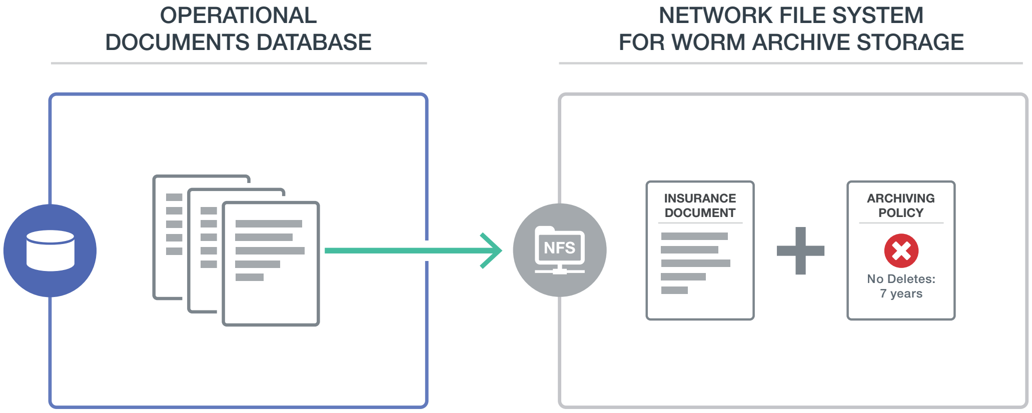
MarkLogic®

Compliance Archive

DATASHEET

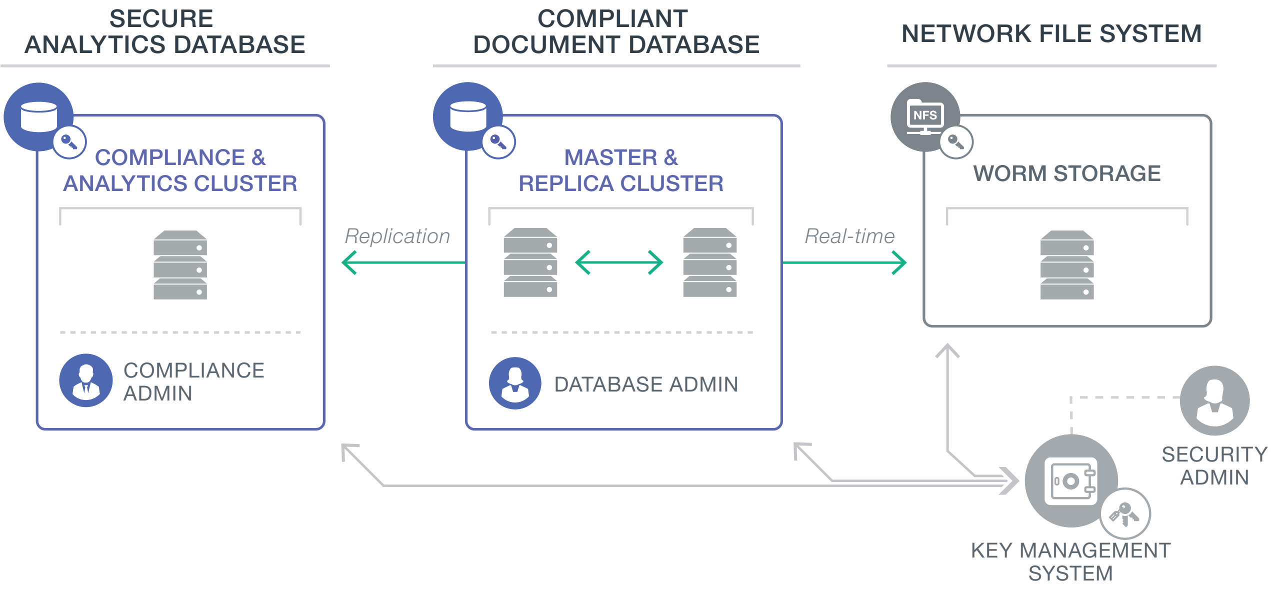
The ability to manage data governance at scale to support e-discovery and legal compliance is a critical business requirement due to regulations such as HIPAA, SEC17a-4, FINRA, and other guidelines for data privacy. The Compliance Archive feature in MarkLogic® helps meet the guidelines for document retention, accuracy, and availability—while not hampering the ability to cost-effectively scale your system and search your data. Compliance Archive achieves this by providing an out-of-the-box mechanism to protect temporal documents against deletion, updates, and wipes using time-based or event-based policies, and save those documents to WORM (Write Once, Read Many) storage with a single operation.


OPERATIONAL DOCUMENTS DATABASE
NETWORK FILE SYSTEM FOR WORM ARCHIVE STORAGE
NFS
INSURANCE DOCUMENT
ARCHIVING POLICY
No Deletes: 7 years

A Smarter Way to Archive Data

Compliance Archive makes it possible to protect and encrypt temporal documents in MarkLogic, such as important insurance documents, financial trades, or other sensitive data, and at the same time save them to WORM storage. MarkLogic's solution preserves your ability to quickly access your data, cost-effectively scale, and maintain data security by taking full advantage of MarkLogic's advanced enterprise capabilities. With MarkLogic's Compliance Archive solution, you can:

- Choose the appropriate temporal versioning (uni-temporal or bitemporal) according to your business needs
- Protect and copy to WORM storage using a single operation
- Send audit copies to WORM storage based on document metadata
- Ensure that queries are tamper-proof and reflect the information as it was inserted by the application
- Ensure that documents are not deleted or tampered with (even by DBAs and system administrators)
- Ensure that temporal versions of documents have immutable URIs (document keys)
- Provide traceability by using protection combined with encrypted audit logs
- Continue to run the database on widely available read-write storage, including DAS (Direct Attached Storage)
- Ensure that documents are permanently archived and can be recovered in case of file system failure or malicious file deletion
- Continue to have lightning fast performance for search and query across your data



Compliance Archive Architecture

Operational Documents Database

A MarkLogic documents database stores your master data, and it runs on commodity read/write storage. Data in this operational database is fully compliant with today's data governance requirements. Data is encrypted, can be secured at the sub-document level, and can have retention clocks applied to prevent wipes, deletes, and updates (e.g., no deletes for 7 years).

Compliance Analytics Cluster

This is an optional part of the architecture, specifically designed for secure analytics. It provides a security administrator full control and visibility, and the ability to create alerting rules to identify malicious activity.

WORM Storage

Data is copied and saved to WORM Storage, utilizing a Network File System (NFS). The data is encrypted by the storage vendor, can be hashed on load for additional security, and can also be audited through MarkLogic.

Key Management System

MarkLogic integrates well with external Key Managements Systems that can be used for advanced encryption. With an external KMS, a security administrator controls access so that even DBAs and compliance administrators cannot tamper with the data.

About MarkLogic

MarkLogic is the world's best database for integrating data from silos, providing an operational and transactional Enterprise NoSQL database platform that integrates data better, faster, with less cost. Visit www.marklogic.com for more information.

MARKLOGIC CORPORATION
999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885 | www.marklogic.com | sales@marklogic.com