

EMC DATA DOMAIN RETENTION LOCK SOFTWARE

Data integrity and secure data retention for archive data

ESSENTIALS

Data Domain Retention Lock Governance Edition

- Satisfy IT governance policies for retaining archive data on a deduplication storage system in a non-rewriteable and non-erasable format
- Set data retention attributes on a file-by-file basis
- Quickly address changing retention policies

Data Domain Retention Lock Compliance Edition

- Dual sign-on ensures protection of archived files from overwrite or deletion
- Efficiently replicate compliant archive data to meet duplicate copy requirements
- Meets the secure retention requirements of a broad list of both U.S. and International compliance standards

Consolidate both governance and compliance archive data

- Consolidate different types of archive data on the same Data Domain system
- Co-locate both backup and archive data on the same Data Domain system

Application Interoperability

- Uses industry-standard protocols for file locking interfaces to ensure broad interoperability
- Integrated with leading file archiving and email archiving applications (EMC SourceOne, Symantec Enterprise Vault, etc.)

Data Integrity

- Inline recovery verification, fault detection, and healing
- Dual disk parity RAID 6

NEXT-GENERATION ARCHIVING

Business-critical data is the foundation for many parts of a company's operations including finance, sales, marketing, and engineering. Ensuring that this data is protected for a long period of time and continues to be easily accessible are key requirements for IT organizations.

As this data is stored and managed in archive storage, IT organizations are required by internal governance policies and regulatory compliance standards (e.g., Security and Exchange Commission for 17a-4 Records (SEC 17a-4(f)), Health Insurance Portability and Accountability Act (HIPAA), etc.) to ensure that these critical business records are retained and unaltered for specific periods of time. Storing this archive data for a long period of time in a cost-effective manner, and enforcing retention policies, are ongoing challenges for IT personnel across many industries.

By deploying EMC® Data Domain® Retention Lock software on EMC Data Domain deduplication storage systems, IT organizations can leverage the industry-leading deduplication storage system to efficiently store and manage backup and archive data. DD Retention Lock ensures that archive data stored on a Data Domain system meets secure data retention requirements driven by either governance policies or by strict regulatory compliance standards.

DATA DOMAIN RETENTION LOCK GOVERNANCE EDITION

DD Retention Lock Governance edition helps you comply with internal IT policies for data retention by making archive data (e.g., files, emails, etc.) non-rewriteable and non-erasable. This ensures that critical business records stored in a Data Domain system are available for retrieval during a specified retention period, at which time the information can be deleted if necessary. The retention period is set on a file-by-file basis, and minimum and maximum retention parameters can be defined for a logical portion of the system to enable more granular management of retention policies. DD Retention Lock Governance lets IT administrators modify time-based retention and other attributes of archive data to adapt to changing business policies for secure data retention.

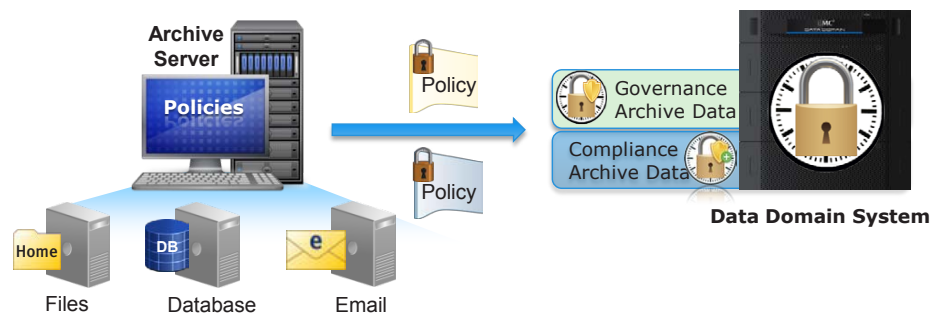
DATA DOMAIN RETENTION LOCK COMPLIANCE EDITION

DD Retention Lock Compliance edition meets the strictest retention requirements of regulatory standards for electronic records such as SEC 17a-4(f). DD Retention Lock Compliance ensures that the files on the Data Domain system that are locked by an archiving application for a specified retention period cannot be deleted or overwritten under any circumstances until the retention period expires. Specifically, when DD Retention Lock Compliance is enabled on a Data Domain system, additional administrative security is provided in the form of "dual" sign-on. This requires that the system administrator as well as another authorized user (also referred to as the "Security Officer") both sign-on to the

system to perform certain administrative functions or actions. This ensures actions that could potentially compromise the integrity of archive data prior to expiration of the retention period are not under the control of a single administrator. This bullet-proof data retention solution ensures that the integrity of archived files will not be compromised prior to expiration of the retention period under any circumstances.

CONSOLIDATE BOTH GOVERNANCE AND COMPLIANCE ARCHIVE DATA

DD Retention Lock enables secure file locking of archive data at an individual file level; enabling these files to be intermixed with unlocked files on the same Data Domain system. In addition, both governance and compliance archive data can be stored on the same Data Domain system thus allowing consolidation of the varied sets of data retention requirements for different types of archive data, yielding a better return on investment and simplified management.



Archiving on EMC Data Domain deduplication storage systems

Co-locate both backup and archive data on a Data Domain system using multiple retention policies. Use DD Retention Lock Governance to securely retain data per corporate governance policies. Use DD Retention Lock Compliance to meet the strictest data retention requirements for regulatory compliance.

TECHNICAL ASSESSMENT AND COMPLIANCE STANDARDS

EMC engaged Cohasset Associates, an industry-leading records management consulting firm, to gain an independent and thorough technical assessment of the capabilities of the DD Retention Lock Compliance relative to meeting the strict requirements set forth in SEC Rule 17a-4(f).

Cohasset Associates performed extensive technical due diligence on the features and functionality available via the DD Retention Lock Compliance, and concluded that the software meets the relevant requirements of SEC 17a-4(f). Specifically, during the SEC required retention period, DD Retention Lock Compliance:

- Provides the integrated control codes and record file management capabilities that ensure protection of record files from overwrite or erasure.
- Provides for initial and ongoing accuracy and quality of the stored records.
- Uniquely identifies each record file and duplicate copy.
- Provides for a duplicate copy of the record files and recovery from the duplicate copy if required.

In addition to meeting the compliance standards for electronic records of SEC 17a-4(f), Data Domain Retention Lock Compliance also meets a broad list of compliance standards for electronic records worldwide across industry verticals such as financial services, healthcare, legal/law, etc. Along with SEC 17-a4(f) and HIPAA, in the U.S., DD Retention Lock Compliance meets the majority of compliance standards including Sarbanes Oxley Act (SOX), Commodity

Futures Trading Commission (CFTC Rule 1.31b), and Food and Drug Administration (FDA 21CFR Part 11). Internationally, DD Retention Lock Compliance meets the compliance requirements of ISO Standard 15489-1 and Model Requirements for the Management of Electronic Records (MoREQ 2).

APPLICATION INTEROPERABILITY

DD Retention Lock software leverages industry-standard management protocols (such as NFS and CIFS) for time-based retention of files. As a result, it can be integrated seamlessly with industry-leading file archiving and email archiving applications including EMC SourceOne™ and Symantec Enterprise Vault, providing an end-to-end archiving solution.

STORAGE EFFICIENCY FOR BACKUP AND ARCHIVE DATA

Unlike traditional disk systems or tape, or other purpose-built solutions, Data Domain systems provide deduplicated self-protecting storage for a broad spectrum of applications. Data Domain inline deduplication technology can yield up to an 80 percent space savings for long-term email and file archives, so enterprises can dramatically reduce the amount of required storage capacity, data center space, and power and cooling—lowering total cost of ownership (TCO) over the lifecycle of the data.

INDUSTRY-LEADING TECHNOLOGY

Data Domain systems provide integrated, deduplicated snapshots for efficiently storing point-in-time versions of backup and archive data. Data Domain systems can also efficiently replicate both the archive data and the data retention settings (e.g., minimum and maximum retention period) to a secondary site, providing DR capabilities for the archived data. EMC Data Domain Replicator software transfers only unique data to facilitate up to a 99 percent reduction in the bandwidth required, while enabling fast “time-to-DR” readiness.

ULTIMATE DATA INTEGRITY

To fulfill stringent compliance standards, it is critical that an archive solution meets the SEC Compliance Requirement 17a-4(f)(2)(ii)(B) which states that the solution must “verify accurately the quality and accuracy of the recording process.” The EMC Data Domain Data Invulnerability Architecture enables DD Retention Lock to meet this requirement by providing the industry’s best defense against data integrity issues.

Inline write and read verification protects against, and automatically recovers from, data integrity issues during data ingest and retrieval. Capturing and correcting I/O errors inline during the backup process eliminates the need to repeat backup jobs, ensuring backups complete on time and satisfy service-level agreements. Unlike other enterprise arrays or file systems, continuous fault detection and self-healing features protect data throughout its lifecycle on all Data Domain systems.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com.

EMC², EMC, Data Domain, SourceOne, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. © Copyright 2011, 2012 EMC Corporation. All rights reserved. Published in the USA. 05/12 Data Sheet H6806.5

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.