

EMC DATA DOMAIN ENCRYPTION SOFTWARE

Secure encryption of data-at-rest

ESSENTIALS

Secure Data Management

- Encrypt all data stored on a Data Domain deduplication storage system
- Protect data from theft or loss of system, disk shelves, disks, or factory returned disks
- Implement encryption to satisfy internal governance rules and compliance regulations
- Meet compliance needs using industry standard AES-128 or AES-256 encryption algorithms
- Uses RSA BSAFE FIPS 140-2 validated cryptographic libraries

Inline Encryption

- Realtime, immediate data encryption
- SISL architecture leveraged for optimized encryption
- Software-based encryption controls costs

Key Management and Integrity

- Integrated with RSA Data Protection Manager for centralized encryption key lifecycle management
- Robust protection against accidental key loss
- Passphrase protection of encryption keys

Easy Integration

- Supports leading backup and archive applications
- Encrypts data ingested via EMC Data Domain Boost, VTL, CIFS, NFS, and NDMP
- Works with EMC Data Domain Replicator and EMC Data Domain Retention Lock software

ADVANCED ENCRYPTION FOR BACKUP AND ARCHIVE DATA

The proliferation of publicized data loss, coupled with new governance and compliance regulations, is driving the need for customers to encrypt their data-at-rest. EMC® Data Domain® Encryption software provides a way for organizations to enhance the security of their backup and archive data that resides on their EMC Data Domain deduplication storage systems using RSA® BSAFE® FIPS 140-2 validated cryptographic libraries.

Centralized encryption key lifecycle management is also becoming a mandate from many security offices. To meet this requirement, you can use a Data Domain system with RSA Data Protection Manager, which delivers a robust, encryption key lifecycle management solution for the entire enterprise.

SECURE DATA MANAGEMENT

Data Domain Encryption software encrypts all incoming data to ensure it cannot be accessed on the existing system or in any other environment without authenticating and decrypting it. Encrypting data-at-rest satisfies some aspects of internal governance rules and compliance regulations. It protects user data against theft of a Data Domain system, loss of the physical storage media during transit, and eliminates accidental exposure during the replacement of failed drives.

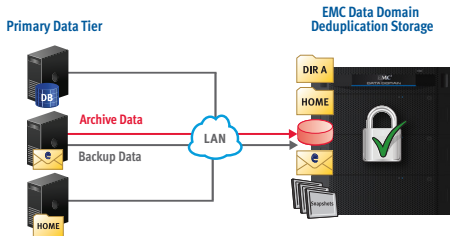
DD Encryption provides administrator selectable, industry-standard 128-bit or 256-bit Advanced Encryption Standard (AES) algorithms implemented by the FIPS 140-2 validated RSA BSAFE cryptographic libraries for encrypting and decrypting all data within the system. Depending on IT security policies, the block cipher modes for the AES algorithm can be set to provide confidentiality using Cipher Block Chaining (CBC) or both confidentiality and message authenticity using Galios/Counter Mode (GCM).

INLINE ENCRYPTION

DD Encryption seamlessly integrates with the high-speed, inline deduplication process used in Data Domain deduplication storage systems, and encrypts data before it is written to disk. Similar to the advantages of inline deduplication, inline encryption requires minimal resources to provide fast, reliable, and secure encryption of backup and archive data.

The combined benefits of inline deduplication and encryption can be realized by simply licensing and enabling DD Encryption on the Data Domain system. Inline encryption provides a faster and more secure solution versus other encryption options because data never resides in a vulnerable, unencrypted state on the disk subsystem.

Unlike other encryption solutions that require additional hardware resources or processing power, DD Encryption requires no additional hardware and has only moderate impact on



EMC Data Domain Inline Encryption

DD Encryption seamlessly integrates with the high-speed, inline deduplication process used in Data Domain deduplication storage systems, and encrypts data before it is written to disk. Similar to the advantages of inline deduplication, inline encryption requires minimal resources to provide fast, reliable, and secure backup and recovery.

performance. By leveraging the EMC Data Domain Stream-Informed Segment Layout (SISL™) scaling architecture, duplicate segments require no encryption processing. This optimization results in much lower resource consumption by the encryption process, thereby lessening the impact on overall performance. This also eliminates additional servers or appliances for encryption in the infrastructure.

KEY MANAGEMENT AND INTEGRITY

Data Domain Encryption software by default encrypts all the data on the system using an internally-generated encryption key. This key is static and cannot be changed by the user. For environments requiring encryption keys to be changed on a periodic basis to meet compliance regulations, RSA Data Protection Manager (RSA DPM) can manage the lifecycle of the encryption key for each Data Domain system. Policies to rotate the encryption key on a periodic basis can be centrally configured using RSA DPM. Keys can also be deleted, expired, or marked as compromised when there is a possibility of a data breach. To further ensure that the encryption keys are safeguarded, a copy of each key can be stored in a second RSA DPM server. In addition, RSA DPM provides audit logs for key state changes that are necessary to prove compliance.

For flexibility in selecting the appropriate encryption methodology, it is possible to use the static encryption key on some Data Domain systems, and the encryption key rotation via RSA DPM on other Data Domain systems in the same environment.

Data Domain systems have one active encryption key for data being written to the system. To provide an additional level of security, an access passphrase is used to encrypt the encryption key when storing it on the Data Domain system. This allows a Data Domain system to be safely shipped with encrypted data and the encryption key without fear of compromising the integrity of the encryption key.

EASY INTEGRATION

DD Encryption supports leading enterprise backup and archive applications and easily integrates into existing enterprise infrastructures. Additional deployment flexibility exists with support for multiple simultaneous data access methods including the use of EMC Data Domain Virtual Tape Library software over Fibre Channel, or NFS and CIFS file service protocols over Ethernet, or as a disk-based target using application-specific interfaces such as EMC Data Domain Boost.

DD Encryption greatly simplifies encryption management since the encryption process is done on the Data Domain system and is completely transparent to the applications writing to it. This allows flexibility in selecting and changing applications without impacting the encryption process. In addition, multiple backup and archiving applications can concurrently access the Data Domain system.

DD Replicator can be used in conjunction with DD Encryption enabling the replication of encrypted data over the network. To further improve security for data being transferred over the network, DD Replicator provides encryption of data-in-flight. Likewise, file and email archive data secured using EMC Data Domain Retention Lock software can also be stored and replicated in an encrypted form.

SPECIFICATIONS

SOFTWARE

EMC Data Domain Operating System 4.9 or later (DD Encryption)

EMC Data Domain Operating System 5.2 or later (RSA Data Protection Manager integration)

RSA Data Protection Manager 2.7, 3.1

EMC Data Domain Boost software

EMC Data Domain Replicator software

EMC Data Domain Retention Lock software

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, Avamar, Data Domain, Global Compression, NetWorker, RSA, BSAFE, SISL, the EMC logo, and the RSA 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 H7028.4

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

EMC Backup Recovery Systems
Santa Clara, California
95054
1-408-980-4800
In North America 1-866-933-3873

EMC²[®]