EMC DATA DOMAIN ENCRYPTION SOFTWARE

Secure encryption of deduplicated backup and archive data

NEXT-GENERATION DATA PROTECTION

EMC® Data Domain® deduplication storage systems have revolutionized backup, archiving, networked disaster recovery, and remote office data protection with high-speed, inline deduplication. This enables the simplest approach to minimizing, and in some cases eliminating, the use of tape for operational recovery and longer term retention.

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 data that resides on their Data Domain systems using industry-standard encryption algorithms.

SECURE DATA MANAGEMENT

DD Encryption encrypts all incoming data to ensure it cannot be accessed on the existing system or in any other environment without first successfully 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 backup and recovery.

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 performance. By leveraging the EMC Data Domain 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.

EMC²

Primary Data Tier

EMC Data Domain Deduplication Storage

Archive Data

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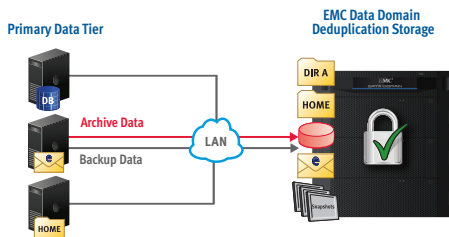
EMC Data Domain Inline Encryption
DD Encryption seamlessly integrates with the high-speed, inline deduplication process used in Data Domain deduplication storage systems, and encrypts data before it is written to disk. Similar to the advantages of inline deduplication, inline encryption requires minimal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

KEY MANAGEMENT AND DATA INTEGRITY

Basic key management functions combine simplicity with ease of use to provide data security at the appropriate level. The Data Domain system has one encryption key for all data on the system thereby making key management simpler. For reliability and security, the encryption key is also protected and stored encrypted. The EMC Data Domain Data Invulnerability Architecture with RAID 6 data protection safeguards the reliability and recoverability of the data and assures recoverability of the encryption key. Checksums and continuous end-to-end data integrity verification provide additional safeguards.

For additional protection and flexibility, the system key is encrypted using an access passphrase. This allows the access passphrase to change without changing the system encryption key providing consistent key management in the event of employee turnover. Additionally, it allows a Data Domain system to be shipped safely with encrypted data and the encryption key, but without the access passphrase on the system.

EASY INTEGRATION

DD Encryption supports leading enterprise backup and archive software 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, through NFS and CIFS file service protocols over Ethernet, or as a disk-based target using application-specific interfaces such as EMC Data Domain Boost (for use with EMC NetWorker®, EMC Avamar®, and Symantec OpenStorage).

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

EMC Data Domain Replicator software can be used in conjunction with DD Encryption enabling the replication of encrypted data over flexible replication topologies. This improves security for data being transferred over the network. Likewise, files locked using EMC Data Domain Retention Lock can be stored encrypted and replicated.

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®