cpl.thalesgroup.com

THALES

Dell EMC PowerProtect DD and Thales CipherTrust Manager for Data-at-Rest and Data Replication Encryption

Encryption is fundamental to any data defense strategy, regardless of whether the end goal is regulatory compliance or securing sensitive data. Self-encrypting drives are an effective way to automatically enforce encryption in storage deployments.

However, as the number of data storages appliances (backup systems, physical storage devices, and number of replicated copies) increases, so do the number of encryption keys, key stores, and associated access policies needing management. The resulting administrative effort involved in managing the encryption deployments and the associated key lifecycle is significant, and can become unwieldy as encryption use increases. To cost-effectively support such an environment and bring it into regulatory compliance, enterprise key management must be part of the solution.

Solution

Centralizing the storage of encryption keys not only simplifies key management, but also ensures that encrypted data is protected from unauthorized access—even as the size of the encryption deployment grows. Dell EMC data-at-rest encryption and encryption of data-in-flight combine to protect sensitive backup data within and between Data Domain systems. Thales CipherTrust Manager is a physical or virtual key manager that integrates with Dell EMC Data Domain solutions to provide robust, enterprise-scale key management, ensuring that encryption keys are kept separate from where the data resides, and are managed throughout their lifecycle and properly secured with FIPS 140-2 compliant solution.

Dell EMC Data Domain Encryption

Data Domain systems, as central repositories for both structured and unstructured backup data, have many security capabilities and attributes to protect the data stored inside them. A Data Domain system provides the ability to encrypt both data at rest and data that is being replicated between systems. Encryption of data at rest protects user data in the situation where a Data Domain system is lost or stolen and eliminates accidental exposure if a failed drive requires replacement. When the file system is intentionally locked, an intruder who circumvents network security controls and gains access to the Data Domain system will be unable to read the file system without the proper administrative control, passphrase, and cryptographic key. When Data Domain Encryption is enabled, the system randomly generates a single, static system-wide cryptographic strength encryption key. Data Domain Encryption software is completely transparent to the backup or archive application, and comes with the Data Domain Operating System that powers all Data Domain platforms.

Data Domain Encryption provides inline encryption, along with Dell EMC's advanced inline deduplication. This means as data is being ingested, the stream is de-duplicated, compressed, and encrypted using an encryption key before being written to the RAID group. Data Domain Encryption software uses RSA BSAFE libraries, which are FIPS 140-2 validated.

One of two cipher modes, Cipher Block Chaining mode (CBC) or Galois/Counter mode (GCM), can be selected to best fit security and performance requirements. In addition, the system leverages a user-defined passphrase to encrypt that key before it is stored in multiple locations on disk. The system encryption key cannot be changed and is not, in any way, accessible to a user. Without the passphrase, the Data Domain file system cannot be unlocked, thus data is not accessible. With CipherTrust Manager, the Data Domain system will use 256-bit Advanced Encryption Standard (AES) algorithm for encrypting all data within the system.

CipherTrust Manager

Thales CipherTrust Manager is an encryption and key management appliance that centralizes the control of an enterprise's disparate encryption solutions. CipherTrust Manager integrates with Dell EMC Data Domain via the Key Management Interoperability Protocol (KMIP) to store the encryption keys. By consolidating the policy and key management of application servers, databases, and file servers, security administration is streamlined. Centralized key management improves security in a number of ways, most notably by making key surveillance, rotation, and deletion easier, while also separating duties so that no single administrator is responsible for the entire environment. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible which, in turn, makes demonstrating compliance with data governance requirements simple.

Features and Benefits of CipherTrust Manager in Dell EMC Backup Environments

Centralize Management of Encryption Keys

Centralize and simplify key management (e.g., key generation, escrow, recovery) for all Dell EMC Data Domain systems and other KMIP-compatible encryption solutions, while improving compliance and auditability.

Disparate encryption solutions lead to key management silos, each with its own discrete enforcement policy. CipherTrust Manager's support for the KMIP protocol enables it to centralize and simplify key management for the entire Dell EMC Data Domain infrastructure while removing the challenge of ongoing maintenance, management, and auditability associated with disparate encryption solutions. Additionally, CipherTrust Manager can centralize encryption keys for third-party KMIP-compatible encryption solutions that may be a part of the enterprise's overall security posture.

Enable Multi-Tenant Data Isolation

In multi-tenant environments, where storage is shared across the Dell EMC infrastructure, granular key administration allows for the co-mingling of data without exposing it to unauthorized users. CipherTrust Manager enables granular user authorization based on defined access and usage policies, and can automatically retrieve administrator, security, and user access controls from existing LDAP or Active Directory services.

Share storage resources while securing data by business policy to segregate data for multiple departments, business units, or customers.

Ensure Root of Trust

Distributed storage can make data access control more challenging. Meeting compliance mandates in these environments is simplified through verifiable and auditable enterprise key management. Data may reside locally, remotely, or virtually within the Data Domain infrastructure. However, the keys and user access controls are secured within CipherTrust Manager, which remains under your security team's control, not the storage administrators.

Enable Separation of Administrative Duties

CipherTrust Manager supports granular authorization, enabling constraints to be placed on specific key permissions to protect against insider threats (For example, only allowing members of the HR department access to employee PII). This is achieved through segmented key ownership based on individuals or group owners. Ongoing storage management occurs as always; however, storage administrators cannot gain access to sensitive data unless they are also entrusted by policy with access to the encryption keys.

Maximize Security

CipherTrust Manager centralizes all key management activities, including key signing, role based administration, quorum control, and the backup and distribution of encryption keys enterprise-wide. For sensitive security operations, you can stipulate multiple credential authorization from multiple administrators.

Resiliency and High Availability

Multiple CipherTrust Manager appliances can be clustered for high availability, with configuration information replicated instantly between members to dramatically improve failover capabilities and fault resiliency for geographically dispersed data center deployments.

Cluster multiple CipherTrust Manager appliances to maintain encrypted data availability, even in geographically dispersed data centers.

Auditing, Logging, and Alerting

CipherTrust Manager's built-in auditing, logging, and alerting functions facilitate regulatory compliance for your entire Dell environment. All keys, certificates, and passwords are securely managed, key ownership is clearly defined, and key lifecycle management is logged to provide a non-repudiative audit trail.

Simplified Key Destruction

Centralized key management simplifies disposing of keys when data is retired or replaced, or the integrity of the key has been weakened or compromised. Administrators can easily manage keys without accessing individual hardware or software appliances to ensure that data has been rendered unreadable, in the event that the appliance is repurposed, destruction of the data is required, or if the key has been compromised.

Conclusion

Encrypting data in the backup environment is critical to ensuring that data is safe in the event of a security breach.

Dell EMC and Thales combine to offer organizations the ability to secure data through encryption without making the management of the necessary encryption keys and policies unwieldy or difficult.

To learn more, visit cpl.thalesgroup.com/partners/dell-emc

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.