gemalto
security to be free

SOLUTION BRIEF

Dell Compellent and Gemalto SafeNet KeySecure for Dell Self-Encrypting Drives

Encryption is fundamental to any defense-in-depth strategy, regardless of whether the end goal is regulatory compliance or securing sensitive data. Self-encrypting drives are an effective way to deploy encryption in storage deployments. However, as the number of drives increases, so does the number of encryption keys, key stores, and associated access policies needing management. The 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, centralized 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 Compellent self-encrypting drives ensure that data stored on those drives is secure. SafeNet KeySecure by Gemalto integrates with Dell Compellent solutions to provide robust, enterprise-scale key management, ensuring that encryption keys are managed throughout their lifecycle and properly secured with FIPS 140-2 certified hardware.

Dell Compellent

The Dell Compellent storage system optimizes data throughout its lifecycle via built-in intelligence that automatically places data on drives according to its level of use. Dell Compellent is a high-performance, efficient, and scalable storage platform based on a modular architecture that unifies block and file, and helps lower total cost of ownership. Real-time system information about each data block allows Dell Compellent's Storage Center to optimize data placement, management, and protection throughout the lifecycle. In addition, Dell Compellent secures data from unauthorized access through the use of FIPS 140-2 Level 2-compliant self-encrypting drives using the Advanced Encryption Standard (AES) algorithm.

Key Benefits

Centralize Management of Encryption Keys

> Centralize and simplify key management (e.g., key generation, escrow, recovery) for all Dell Compellent self-encrypting drives and other KMIP-compatible encryption solutions, while improving compliance and auditability.

Multi-Tenant Data Isolation

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

High-Availability Configurations

> Cluster multiple SafeNet KeySecure appliances to maintain encrypted data availability, even in geographically dispersed data centers.

Separation of Duties

> SafeNet KeySecure by Gemalto supports segmented key ownership and management based on individuals or group owners. This approach is perfect for protecting sensitive material against unauthorized access from staff.

SafeNet KeySecure

SafeNet KeySecure by Gemalto is an encryption and key management appliance that centralizes the control of an enterprise's disparate encryption solutions. KeySecure integrates with Dell Compellent via the Key Management Interoperability Protocol (KMIP) to store the encryption keys for each self-encrypting drive. 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.

Key features

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

Ensure Root of Trust

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

Enable Multi-Tenant Data Isolation

In multi-tenant environments, where storage is shared across the Dell infrastructure, granular key administration allows for the co-mingling of data without exposing it to unauthorized users. KeySecure 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.

Enable Separation of Administrative Duties

SafeNet KeySecure by Gemalto 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.

Benefits of KeySecure in Dell Storage Environments

Maximize Security

- SafeNet KeySecure by Gemalto 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 SafeNet KeySecure 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.

Auditing, Logging, and Alerting

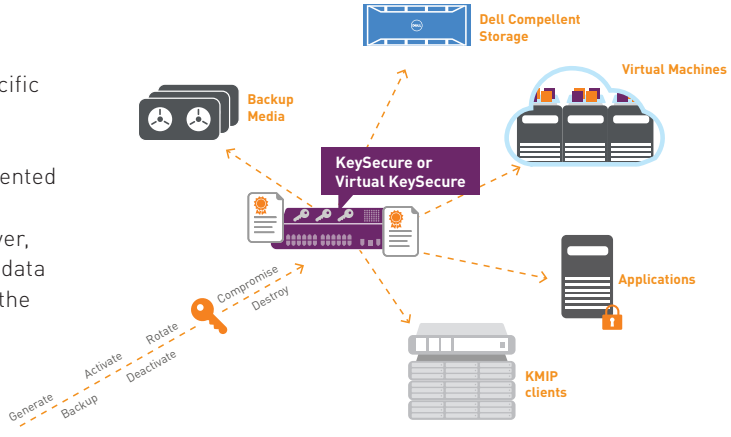
- SafeNet KeySecure's built-in auditing, logging, and alerting functions facilitate regulatory compliance for your entire Dell environment. All keys, certificates, and passwords are securely managed, key ownership is clearly defined, and key lifecycle management is logged to provide a non-repudiative 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 storage environment is critical to ensuring that data is safe in the event of a security breach. Dell and SafeNet key management solutions by Gemalto 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 www.safenet-inc.com/partners/dell



Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free