Technology Partner

Dell and SafeNet: Key Management for Enhanced Encryption Security

SafeNet KeySecure secures Access Keys in hardware, and streamlines management to serve as a root of trust for encryption deployments in Dell Compellent deployments.

- **Centrally Manage Access Keys** - Centralize and simplify key management (e.g., key generation, escrow, recovery) functions to reduce administrative overhead and improve 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 KeySecure appliances to maintain encrypted data availability, even in geographically-dispersed data centers.
- **Separate duties** - Segment key ownership and management based on individuals or group owners. This approach is perfect for protecting sensitive material against unauthorized access from staff.

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 large-scale storage deployments. However, as the number of drives increases, so too 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™ integrates with Compellent Secure Data solutions to provide robust, enterprise-scale key management, ensuring that encryption keys are managed throughout their lifecycle and properly secured with up to FIPS 140-2 Level 3-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. 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 Compellent's Storage Center to optimize data placement, management, and protection throughout the lifecycle. In addition, 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.

SafeNet KeySecure

KeySecure is a 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 Authority Credentials (sometimes referred to as the locking keys, authentication keys or Access Keys) for each self-encrypting drive. By consolidating the policy and key management of application servers, databases, and file servers, it streamlines security administration. 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 Access Keys
Disparate encryption solutions lead to key management silos, each with its discrete enforcement policy. 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 KeySecure, which remains under the control of your security team, 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
KeySecure supports granular authorization, enabling constraints to be placed on specific key permissions to protect against insider threats. 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.

Conclusion:

To learn more, visit:
http://www.safenet-inc.com/partners/dell/

About SafeNet
Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high-value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

The Dell Technology Partner Program
SafeNet is a Dell Technology Partner. KeySecure is certified by Dell to run on the Dell platforms specified in the technical architecture section.

The Dell Technology Partner program is a multi-tier program that includes ISVs, IHVs and Solution Providers. This global program helps partners build innovative and competitive business solutions using Dell platforms. Program resources keep customer costs low and help to sustain competitiveness.

The program has a structured and streamlined process that combines technology and business strategies with Dell Solution Center expertise to on-board and test partner products on Dell platforms. This testing process helps ensure that products have met the technical requirements to perform well on Dell platforms.