Solution Brief

Gemalto and NetApp: Securing Network-Attached Storage with SafeNet KeySecure for Centralized Key Management

Key Benefits

Centralize Management of Encryption Keys
Centralize and simplify key management for your entire NetApp infrastructure while improving compliance and auditability.

Enable Multi-Tenant Data Isolation
Leverage shared resources while securing data by business policy to segregate data for multiple departments, business units, or customers.

Achieve High Availability
Cluster multiple SafeNet KeySecure appliances to maintain encrypted data availability even in geographically dispersed data centers.

Enable Auditing, Logging, and Alerting
Improve regulatory compliance for your entire NetApp environment with a nonrepudiative audit trail.

The Challenge

Successful encryption implementations are fundamental to addressing regulatory mandates, passing security audits, and protecting sensitive information. However, the growing number of encryption keys and associated key stores across multiple storage tiers and vendor platforms—deployed within primary, secondary, and even cloud-based data centers—often result in uncontrolled management complexity. As security teams struggle to keep pace with the administrative effort of managing encryption deployments and key lifecycle operations, many organizations are evaluating ways to increase productivity.

Implementing a unified key management solution provides organizations with significant operational improvements. Enterprise key management—a centralized repository that manages all encryption keys and data access policies across the enterprise—is an effective approach to securing encrypted data from unauthorized access while simplifying the management of keys for all encryption solutions deployed.

The Solution

Partnering with Gemalto, NetApp offers a comprehensive storage security portfolio that delivers encryption flexibility, increases efficiencies, and reduces risk of theft or unauthorized access to stored information. Organizations benefit from a network storage environment that delivers the unique features of the clustered Data ONTAP® operating system combined with Gemalto SafeNet KeySecure™ enterprise key management to make sure that encrypted data remains available at all times for your users and important workloads.

SafeNet KeySecure simplifies the challenges of managing encryption keys, making sure keys are secure and information is available to authorized users within your NetApp storage infrastructure. With KeySecure, administrators can simultaneously manage keys associated with NetApp Storage Encryption (NSE), Gemalto SafeNet StorageSecure data encryption, and other KMIP-based encryption solutions. This centralized approach to key management helps security teams streamline operations, effectively secure physical, virtual, and private cloud-based environments, and enforce security policies regarding access and use.

With clustered Data ONTAP, you have access to NetApp's storage efficiency technologies, including Snapshot™ copies; thin provisioning; FlexClone®, SnapMirror®, and SnapVault® technologies; deduplication; compression; RAID-DP® technology; and flash, using FAS storage controllers. SafeNet KeySecure maintains data confidentiality on NetApp FAS solutions through efficient centralized key management and by enforcing customized security policies surrounding data access. This combination of a modern

NetApp®

gemalto
security to be free
Security Solutions Partner

storage infrastructure and KeySecure delivers peace of mind that your data and encryption keys are protected against unauthorized access, while making the most efficient use of your storage investments.

Centralize management of encryption keys

Disparate encryption solutions lead to key management silos, each with its discrete enforcement policy. SafeNet KeySecure supports the KMIP protocol, making it possible to centralize and simplify key management for your entire NetApp infrastructure, including SafeNet StorageSecure and NSE deployments, while removing the challenge of ongoing maintenance, management, and auditability associated with disparate encryption solutions.

Ensure root of trust

Distributed or cloud-based storage can introduce challenges to data access control, as data may reside locally, remotely, or virtually within your NetApp infrastructure or private cloud. With SafeNet KeySecure, keys and user access controls are secured within the key management system, which remains under the control of your security team, not the storage administrators. And meeting compliance mandates is greatly simplified with a verifiable and auditable enterprise key management solution.

Enable multi-tenant data isolation

Multi-tenant or private cloud environments require the ability to store data across your shared NetApp infrastructure. Through the use of SafeNet KeySecure's granular key administration, organizations can comingle data without exposing the data to unauthorized users. User authorization is based on defined access and usage policies, and it provides the ability to automatically retrieve administrator, security, and user access controls from existing LDAP or Active Directory® services.

Enable separation of administrative duties

SafeNet KeySecure supports granular authorization, and allows constraints to be placed on specific key permissions to protect against insider threats through segmented key ownership based on individuals or group owners. Ongoing management of your NetApp storage remains the same; however, storage administrators cannot gain access to sensitive data unless they are also entrusted by policy with access to the encryption keys.

Benefits of SafeNet KeySecure in NetApp storage environments

- **Maximized security.** SafeNet KeySecure 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 facilitate regulatory compliance for your entire NetApp environment. All keys, certificates, and passwords are securely managed; key ownership is clearly defined; and key lifecycle management is logged to provide a nonrepudiative 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 and make sure that data has been rendered unreadable in the event the appliance is repurposed, destruction of the data is required, or the key has been compromised.

Partner for Success

NetApp and Gemalto Professional Services offer a wide range of services, including implementation of SafeNet security technologies on the NetApp storage platform. To learn more about data encryption and protection solutions from NetApp and Gemalto, contact your NetApp or Gemalto representative.

Use of the word "partner" or "partnership" does not imply a legal partnership between NetApp and any other company

---

About NetApp

Leading organizations worldwide count on NetApp for software, systems and services to manage and store their data. Customers value our teamwork, expertise and passion for helping them succeed now and into the future.

www.netapp.com