Solution Brief

Gemalto and NetApp: Securing Network-Attached Storage with SafeNet StorageSecure Network-Based Encryption

Key Benefits

Secure Regulated Data
Implement data security mandates across your entire NetApp® storage infrastructure.

Secure Archived Data
Enforce data isolation and protection throughout its lifecycle regardless of the storage tier.

Enable Separation of Duties
Allow storage administrators to manage resources without gaining access to sensitive data.

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

The Challenge

As organizations consolidate data across traditional in-house network storage environments or private cloud deployments to reduce operating costs and increase productivity, the risk of information theft or improper disclosure increases. To guard against unauthorized access to intellectual property and regulated customer data, organizations continue to add layers of security to keep pace with today's sophisticated security breaches and stringent government regulations. In addition, storage security solutions must also address the rapid growth in data, virtualization, and multi-tenancy to protect sensitive information from both external and internal attack, while maintaining both performance and ease of use. To meet these challenges, encryption has become more mainstream, as it secures data from unauthorized access or theft.

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 StorageSecure network-based encryption to make sure that encrypted data remains secure and available at all times for users and critical workloads.

SafeNet StorageSecure provides organizations with critical capabilities required by security teams to effectively meet governance, compliance, and data protection mandates. Through the use of encryption, organizations can make sure that data is protected and will be unreadable by unauthorized users. This technology secures sensitive data—even if files are copied or disk drives are stolen—to guard against unauthorized access while data is at rest. Without the proper decryption key, the data is undecipherable and is of no value.

With clustered Data ONTAP, you have access to NetApp's storage efficiency technologies, including Snapshot™ copies; thin provisioning; FlexClone®, SnapMirror®, and SnapVault® technologies; RAID-DP® technology; and flash, using FAS storage controllers. SafeNet StorageSecure is a self-contained storage encryption appliance that delivers 256-bit AES encryption to protect data stored in Ethernet-based storage environments (NAS file servers). StorageSecure enables data confidentiality while enforcing customized security policies surrounding its access and use. This combination of a modern storage infrastructure and Gemalto's security appliances deliver peace of mind that your data is protected against unauthorized access while making the most efficient use of your storage investments.

NetApp®

gemalto
security to be free

Security Solutions Partner

Secure regulated data

Securing data at rest is fundamental to protecting regulated data. SafeNet StorageSecure makes sure that sensitive data is encrypted and unreadable without proper authorization. And by combining StorageSecure with Gemalto SafeNet KeySecure™ key management solution, you are able to enforce robust access and key management controls while maintaining data security mandates across your NetApp storage infrastructure.

Secure archived data

With the NetApp unified architecture, your primary and archive data stores can coexist within the same infrastructure. Through powerful encryption and access controls, SafeNet StorageSecure enforces data isolation and protection, making it unreadable to unauthorized users, even as it moves across different storage tiers within your clustered environment. After data is encrypted, it remains so through its lifecycle regardless of the tier on which it is stored.

Enable separation of administrative duties

SafeNet StorageSecure enforces isolation and granular access to protected data through a variety of security mechanisms, including multifactor authentication and dual control. Only those authorized to perform a given task can do so. Meanwhile, storage server maintenance and administration can occur without administrators gaining access to sensitive data residing on the servers.

Enable multi-tenant data isolation

NetApp infrastructures often can contain data for multiple departments, business units, or customers. While this provides efficient use of your storage assets, shared resources present a risk of unauthorized exposure to sensitive data. SafeNet StorageSecure encrypts data based on defined business policies to prevent inadvertent access to data. In conjunction with SafeNet KeySecure, the solution can manage up to 1 million unique keys to support data protection and isolation within multitenant or shared environments.

Benefits of SafeNet StorageSecure in NetApp storage environments

- **Ease of deployment.** Encryption can be deployed within NetApp storage environments without disrupting existing resources. There are no hosts to configure or software to install. SafeNet StorageSecure encrypts storage transparently without affecting the user experience.
- **Redundancy and high availability.** SafeNet StorageSecure appliances can be paired in a cluster for high availability. All keys, policies, and configuration information are automatically synchronized between cluster members.
- **Administration and user access controls.** You can integrate SafeNet StorageSecure with directory services, such as LDAP, Microsoft® Active Directory® (AD), NIS, and RADIUS to incorporate existing user access and authentication controls. A dual authorization requirement within StorageSecure can further restrict access to sensitive data and protect against rogue administrators.
- **Quick and secure data destruction.** SafeNet StorageSecure, along with SafeNet KeySecure, makes sure that data has been rendered unreadable in the event the appliance is repurposed or destruction of the data is required.
- **Centralized policy and key management.** SafeNet StorageSecure stores all encryption keys and associated parameters within SafeNet KeySecure—a FIPS 140-2 Level 3 validated key management solution. This enables secure distributed management of StorageSecure keys for centralized key management and control.

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