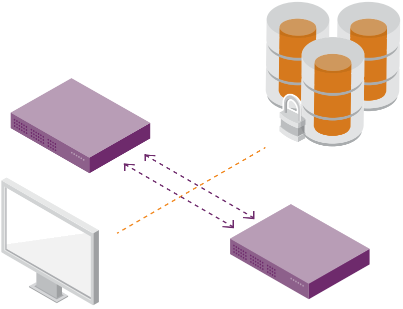
SafeNet | THE DATA PROTECTION COMPANY



StorageSecure and NetApp:

Securing Network-attached Storage

SOLUTION BRIEF

Key Features

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

Storage administrators can 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

Today, it is common to find that organizations are consolidating their data in network storage environments as either traditional in-house or private cloud deployments to reduce operating costs and increase productivity. However, with these operational benefits also comes the risk of information theft or improper disclosure. To guard against unauthorized access to intellectual property and regulated customer data, organizations are adding layers of security. The rapid growth in data, virtualization, and multi-tenancy, combined with increasingly sophisticated security breaches and more stringent government regulations has created new challenges that must be met by a new type of storage security solution. Such a solution must protect sensitive information from both external and internal attacks while maintaining performance and ease of use.

The Solution

Encrypting data at rest—that is, making sure data on a disk is encrypted at all times—is an effective means by which to guard against unauthorized access. Without the proper decryption key, the data is undecipherable and therefore of no value. This approach protects against unauthorized access while supporting granular encryption and user access controls. NetApp and SafeNet have developed a security solution that delivers strong encryption and guards against unauthorized access even while data is at rest.

With NetApp and SafeNet, you can enjoy the benefits of a network storage environment that delivers the unique features of the clustered Data ONTAP® operating system, combined with the data security and protection afforded by SafeNet StorageSecure encryption and SafeNet KeySecure key management.

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 and V-Series storage controllers. StorageSecure is a self-contained storage encryption appliance that delivers 256-bit AES encryption to protect data stored in Ethernet-based (NAS file servers or iSCSI LUNs) storage environments. StorageSecure enables data confidentiality on NetApp FAS or V-Series solutions while enforcing customized security policies surrounding its access and use. This combination of a modern storage infrastructure and SafeNet security appliances delivers the peace of mind that your data is protected against unauthorized access while simultaneously making the most efficient use of your storage investments.

Benefits of StorageSecure in NetApp Storage Environments

Ease of Deployment

- You can deploy encryption into NetApp storage environments without disrupting existing resources. There are no hosts to configure or software to install. StorageSecure encrypts storage transparently without affecting the user experience

Redundancy and High Availability

- StorageSecure appliances can be paired together in a cluster for high availability. All keys, policies, and configuration information is automatically synchronized between cluster members.

Administration and User Access Controls

- You can integrate 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

- StorageSecure, along with KeySecure, makes certain that data has been rendered unreadable in the event the appliance is repurposed or destruction of the data is required.

Seamless Migration

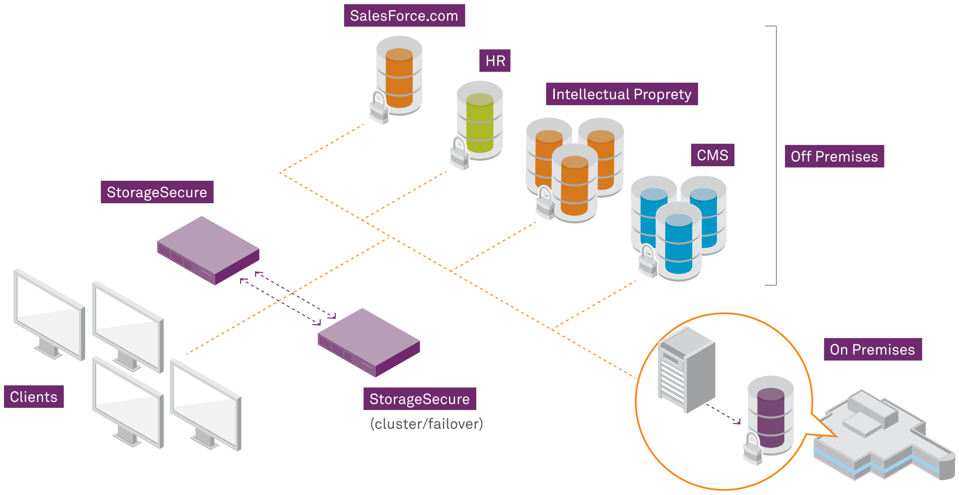
- Many existing DataFort implementations can be migrated to SafeNet StorageSecure. The existing configuration is replicated onto StorageSecure without interruption to data access and user workflow.

Centralized Policy and Key Management

- StorageSecure stores all encryption keys and associated parameters within KeySecure, SafeNet's FIPS 140-2 Level 3-validated key management solution. This enables secure distributed management of StorageSecure keys for centralized key management and control.

Secure Regulated Data

Protecting sensitive data at rest is fundamental to protecting regulated data. StorageSecure makes sure that sensitive data is encrypted and therefore unreadable without authorization. By combining SafeNet StorageSecure and SafeNet KeySecure, 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 archival data stores can coexist within the same infrastructure. Through powerful encryption and access controls, StorageSecure enforces data isolation and protection by rendering it unreadable to unauthorized users, even as it is moves across the different storage tiers within your clustered environment. Once data is encrypted, it remains so through its lifecycle regardless of the tier on which it is stored.

Enable Separation of Administrative Duties

Access to StorageSecure, its administration, and the encryption keys is tightly controlled through a variety of security mechanisms, including multi-factor authentication, ensuring that only authorized administrators can perform certain tasks. Ongoing management of your NetApp storage 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

Enable Multi-Tenant Data Isolation

Your NetApp infrastructure can contain data for multiple departments, business units, or customers. While providing efficient use of your storage assets, shared resources present a risk of unauthorized exposure to sensitive data. StorageSecure encrypts data based on defined business policies so that inadvertent access to data is prevented. In conjunction with SafeNet KeySecure, the solution can manage up to 1 million unique keys to support data protection and isolation within multi-tenant or shared environments.

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