SOLUTION BRIEF

StorageSecure and NDMP Environments

The Challenge

Today, many organizations have embraced storage management solutions based on the Network Data Management Protocol (NDMP). NDMP-compliant solutions provide strong access controls by separating the flow of backup and restore control information from the flow of data to and from backup media. These solutions help organizations achieve enterprise-wide backup of their data assets regardless of where they reside on the network, permitting platforms to be used at a departmental level while handling backup at the enterprise level.

Although NDMP centralizes and simplifies network-based data backup, organizations are increasingly concerned with regulatory compliance that requires data access to be limited to authorized users. With standard backup procedures, data is often "in the clear" or unencrypted. To guard against unauthorized access to intellectual property and regulated customer data, organizations need to secure their data as soon as it is created, regardless of the source application or user. In addition, these solutions 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 that data on a disk is encrypted at all times—is an effective way to guard against unauthorized access. Without the proper decryption key, the data is undecipherable and has no value. This approach protects against unauthorized access while supporting granular encryption and user access controls. The Gemalto SafeNet StorageSecure security solution can easily be added to existing NDMP-based backup environments to deliver the strong encryption needed to guard against unauthorized access to data at rest or during the backup process.

Key Benefits

Total protection
> Secure sensitive data in both online and offline storage, on- and off-premises, at the same time with one solution.

Ease of deployment
> Add StorageSecure into your current NDMP-based backup solution without disrupting existing resources.

Secured backup stream
> Make sure your NDMP backup is encrypted so that sensitive data is unreadable without authorization.

Protection against backup media loss
> Secure your backup media against access even if it is lost or stolen.

NetApp and Gemalto provide significant benefits to network storage environments, combining 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.

- **Clustered Data ONTAP.** Leverage a unified architecture to access NetApp's storage efficiency technologies using FAS and V-Series storage controllers for improved utilization and operational efficiencies.
- **StorageSecure.** 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 on NetApp FAS or V-Series solutions and backup copies, as well while enforcing customized security policies surrounding data access.

Comprehensive Business Continuity

The combination of a modern storage infrastructure and Gemalto security appliances delivers the peace of mind that your data is protected against unauthorized access at all times.

Total protection

The combination of StorageSecure and NDMP in your NetApp environment means that you can secure sensitive data in both online and offline storage, on- or off-premises, simultaneously with the same solution. Your data is securely encrypted at all times.

Ease of deployment

You can easily add StorageSecure into your current storage environment without disrupting existing resources. There are no hosts to configure or software to install. StorageSecure encrypts data transparently without affecting the existing NDMP configuration or backup process. Once the initial encryption or a subsequent rekeying of data has taken place, your NDMP backups will reflect the same encryption, delivering additional security to your data protection solution.

Storage efficiency and data security

With StorageSecure and NetApp storage, your non-sensitive data benefits from storage efficiency while sensitive data can be protected through data security encryption and access controls—all within the same storage platform.

Secured backup stream

When you deploy StorageSecure in your storage environment, your NDMP backup process is encrypted in the same manner as your disk drives, rendering sensitive data unreadable without authorization. This is in contrast to full disk encryption solutions, where the data is encrypted on the disk but travels across the network "in the clear" to the backup device. Depending upon compliance requirements, this extra degree of security may prove very desirable and outweigh the tradeoff of reduced compression when writing to backup media.

Protection against loss or theft of backup media

Since your NDMP backups reflect the same encryption as your primary storage, you are protected against data disclosure even in the event of the theft of other loss of your backup media. Without the correct decryption key that is stored on the KeySecure key manager appliance, the backup media is undecipherable.

Redundancy and high availability

StorageSecure appliances can be paired together in a cluster for high availability. All keys, policies, and configuration information are automatically synchronized between cluster members. This is particularly helpful when backups are housed at remote data center locations.

Administration and user access controls

Access to StorageSecure, its administration, and the encryption keys is tightly controlled through a variety of security mechanisms, including multi-factor authentication and dual authorization, making sure that only authorized administrators can perform certain tasks. This can further restrict access to sensitive data in both primary storage and backups while protecting against rogue administrators. You can integrate StorageSecure with directory services, such as LDAP, Microsoft® Active Directory®, NIS, and RADIUS to incorporate existing user access and authentication controls.

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