SafeNet | THE DATA PROTECTION COMPANY

SafeNet StorageSecure

PRODUCT BRIEF

Benefits

- Ensures data isolation and granular access controls to protected data in shared and virtual environments
- Encrypts data in real-time at the point of capture / creation
- Strengthens existing LDAP, MS AD & NIS controls by adding an additional layer of access controls
- Protects data for compliance mandates
- Protects offline data in archives from unauthorized access or theft
- Encrypts files on SAN attached as well as internal NAS storage
- Integrated with SafeNet KeySecure for centralized policy and key management
- Drop-in upgrade for NetApp E-Series DataFort

Fast, Transparent, Cost-Effective Data Protection throughout the Information Lifecycle

Organizations today are consolidating data in network storage reducing operating costs and increasing administration productivity. However, those benefits also bring an increased risk of information theft, compelling organizations to add additional layers of security to protect their intellectual property and regulated customer data. Explosive growth in data, accelerating trends in virtualization and multi-tenancy, increasingly sophisticated information security breaches, and more stringent government regulations are creating new challenges that must be met by a new type of storage security solution. Such a solution must ensure the protection of sensitive information, even from insiders, while maintaining ease of use.

SafeNet's StorageSecure is a network storage encryption appliance, protecting data at rest. Due to its deployment model, StorageSecure facilitates quick, simple, and cost-effective storage encryption solutions both for initial installation and ongoing operations. StorageSecure ensures the confidentiality of sensitive data whether it resides on NAS file servers or IP SAN storage systems[1]. With StorageSecure, organizations can seamlessly secure physical, virtual, and cloud-based storage while enforcing customized security policies surrounding its access and use. SafeNet StorageSecure encrypts information based on defined business policies and securely stores the information without impacting ongoing operations or reducing availability.

Multi-Tenant Data Isolation

Network-attached storage often contains data for multiple departments, groups, business units or customers. Data co-mingling presents a risk of unauthorized exposure to sensitive data. An all or nothing storage encryption solution is insufficient. Those allowed to access the protected storage will be able to access all of the data. By protecting data at a granular level, instead of enforcing an all or nothing protection solution, organizations are able to enforce data-specific authorization based on user privileges, job responsibilities, and data location. StorageSecure, in combination with SafeNet KeySecure, protects data with unique keys based on the informational value and internal business policies.

Protection of Regulated Data

Protecting sensitive data at rest is fundamental in protecting regulated data. StorageSecure ensures that sensitive data will be encrypted and rendered unreadable to unauthorized users. By combining StorageSecure and SafeNet's KeySecure, organizations are able to enforce more robust access and key management controls while maintaining data protection mandates.

Securing Archived Data

StorageSecure ensures data isolation and granular access to protected data, rendering it unreadable to unauthorized users, even as it is moves across the different storage tiers. Once data is encrypted, it remains encrypted through its lifecycle without any additional intervention.

[1]Available in a future release

SafeNet StorageSecure: Key Features

Security
- NIST FIPS 140-2 Level 3 (validation in process)
- Cryptography:
  - FIPS-PUB 186: AES (key Length: 256) encryption
  - True Random Number Generator (TRNG)
  - Key zeroization on security breach

High Availability and Reliability
- Clustering for full redundancy and automatic failover
- Dual hot-swappable power supplies
- Redundant fans
- Serviceable air filter
- Anti-probing sensors

Options
- S220: 1GbE network interface
- S280:10GbE network interface

Supported Protocols
- CIFS
- NFS

Supported Directory Services
- Microsoft Active Directory
- LDAP
- NIS

StorageSecure Management
- Manage all StorageSecure and KeySecure appliances from a single management console
- Management console uses optional two-factor authentication with role-based Administration
- Quorum-based authentication for sensitive security operations such as recovery, initialization, and establishing trusted relationships

Privileged User Access and Separation of Duties

Whether used for virtual environments, multi-tenancy, or separation of duties, SafeNet StorageSecure ensures isolation and granular access to protected data. Access to StorageSecure, its administration, and the encryption keys is tightly controlled with a variety of security mechanisms, including multi-factor authentication, ensuring that only those authorized to perform a given task can do so. Storage server maintenance and administration can occur without administrators gaining access to sensitive data residing on the servers.

StorageSecure Benefits

- **Ease of Deployment -** SafeNet StorageSecure offers a seamless, non-disruptive deployment that drops into the network between clients and servers, linking them with a high-speed cryptographic path. There are no hosts to configure or software to install. StorageSecure is ready to encrypt and secure storage transparently without any impact on user experience.
- **Centralized Policy and Key Management -** SafeNet StorageSecure is now part of the Data Encryption and Control offering, such that it is fully integrated into the SafeNet crypto foundation, including SafeNet's KeySecure for key management and data access control policy management. Centralized key management eliminates lost and stolen keys preventing information access. KeySecure can host backup keys to StorageSecure devices for disaster recovery and maintain a key archive for all deployed and purged keys.
- **Redundancy and High Availability -** SafeNet StorageSecure appliances can be clustered with all keys, policies, and configuration information automatically synchronized between cluster members. If one appliance goes offline, the second appliance automatically takes over the combined workload, ensuring that vital encrypted data is always available when needed.
- **Administration and User Access Controls -** SafeNet StorageSecure provides the ability to integrate with user common directory services, such as LDAP, Microsoft AD, and NIS to incorporate existing user access and authentication controls. An additional layer of dual authorization control can be defined within the StorageSecure administration console to further restrict access to sensitive data stored in the storage arrays.
- **Segregation of Data -** Whether used for virtual environments, multi-tenancy, or separation of duties, StorageSecure ensures isolation and granular access to protected data.
- **Quick and Secure Data Destruction -** Safenet StorageSecure, along with SafeNet KeySecure key management solution, ensure that stored sensitive data has been rendered unreadable in the event the storage appliance needs to be repurposed or the data needs to be destroyed.

About SafeNet, Inc.

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

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