Alliance
Storage Technologies Inc.

Encryption Technical Overview

The news is filled with stories about security breaches, corporate espionage, hackers and information leaks. Many industries face mandates that require encryption while others consider it a business necessity. Nevertheless, protecting valuable corporate assets has never been more important, especially with the increasing number of industry regulations and the fines imposed for each breach.

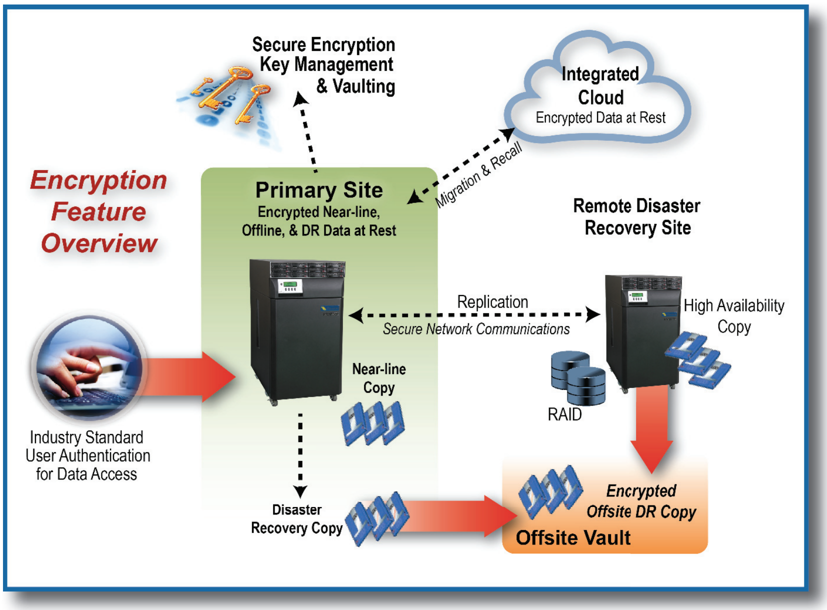
Any sized business or organization that has a requirement for protecting data can benefit from the added security that encryption provides, however, it is especially important to the security and surveillance, legal, government, financial, healthcare and insurance sectors. The Healthcare Information Technology Act (HITECH) requires patient records to be encrypted and levies steep fines for breaches. These far-reaching mandates apply to healthcare institutions, physician's offices, and their business associates which can include insurance companies, financial institutions, or any company dealing with patient records.

- The ASTI data encryption option is enabled through the Archive Management Software (AMS)
- Meets U.S. and Canadian guidelines with FIPS 140-2 compliant, AES 256-bit encryption algorithms
- Encryption applies to all data stored on optical media and Cloud Integrated Storage
- Fileshare partitions are specified for encryption through AMS policies prior to being migrated to optical media or the Cloud
- Symmetric encryption keys for each file are generated and protected by symmetric encryption wrapping keys which are generated via FIPS 140-2 compliant random number generator
- License key management is implemented in accordance with *NIST Special Publication 800-57 Recommendations for Key Management* such that all keys are stored remotely away from the data
- Symmetric Encryption Keys for each data file are protected and stored in an encrypted format utilizing Symmetric Encryption Wrapping Keys for each Archive Volume

Secure valuable data from unauthorized access with ASTI's *Encryption* feature.

Encryption Features and Benefits

- Assures compliance with stringent industry regulations, HIPAA/HITECH, PCI requirements, and more
- Prevents regulatory penalties that could result from a potential breach
- Protects data from unauthorized access due to theft or loss of physical media while in transit
- Safeguards business reputation - the cost of a breach may include loss of customers, class action lawsuits, and damage to brands
- Eliminates the need for third party software (ASTI developer-integrated solution)
- Defends against corporate espionage or malicious attacks
- Secures data silently in the background automatically protecting sensitive data.
- Increases confidence in the security of data stored off-site or in the Cloud
- Prevents against accidental or intentional alteration of data


Encryption Feature Overview
Secure Encryption Key Management & Vaulting
Integrated Cloud
Encrypted Data at Rest
Migration & Recall
Primary Site
Encrypted Near-line, Offline, & DR Data at Rest
Remote Disaster Recovery Site
Replication
Secure Network Communications
High Availability Copy
Near-line Copy
RAID
Industry Standard User Authentication for Data Access
Disaster Recovery Copy
Encrypted Offsite DR Copy
Offsite Vault

Technical Specifications

FIPS 140-2 Compliant Data Encryption

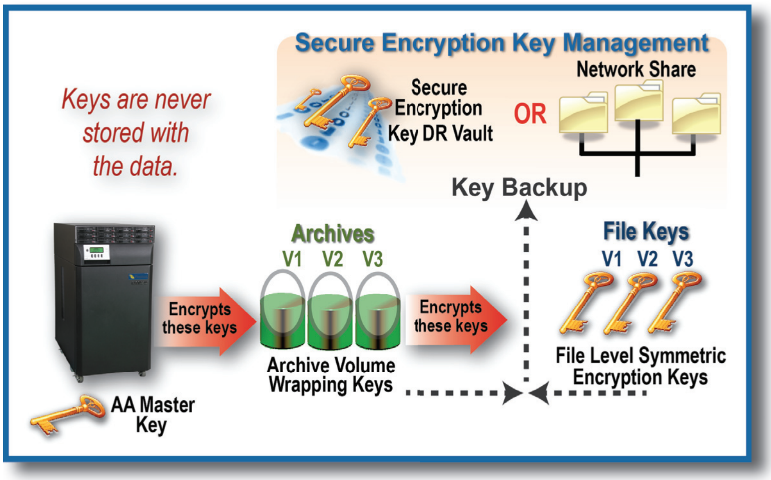
- Meets U.S. and Canadian data encryption FIPS 140-2 guidelines.
- ASTI's Archive Management Software utilizes an embedded FIPS 140-2 validated cryptographic module registered under security certificate #1747 running on a Linux 3.2 platform, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

AES 256-bit Symmetric Encryption Algorithms

- Utilizes Advance Encryption Standard (AES) algorithm specifications established by the U.S. National Institute of Technology (NIST) for electronic data to be retained past the year 2031.
- Utilizes Symmetrical Encryption Keys in a closed system, ensuring no keys are ever externally published or distributed for data access.

Simple Policy Driven Encryption

- Policies and processes are implemented to protect files from alteration or destruction.
- Simple policies defined at the fileshare partition enable data encryption for all data in the archive. If a fileshare partition contains data that must be secured, encryption can be enabled.
- Users and administrators cannot override or circumvent policies. Once the policy is established, all data is encrypted ensuring compliance and protection of data, meeting regulatory mandates.
- All data is securely encrypted utilizing unique keys for each file archived.


Secure Encryption Key Management
Keys are never stored with the data.
Secure Encryption Key DR Vault
OR
Network Share
Key Backup
Archives
V1 V2 V3
File Keys
V1 V2 V3
Encrypts these keys
Encrypts these keys
Archive Volume Wrapping Keys
File Level Symmetric Encryption Keys
AA Master Key

Managers, officers, CIO's and IT administrators can be confident and assured that critical data is secure, protected, and shielded from unauthorized access with the ASTI encryption feature.

Integrated Secure Encryption Key Management

- Adheres to NIST Special Publication 800-57 Guidelines for Key Management preventing unauthorized access and protecting data assets.
- Master Keys protect all other encryption keys in use within the Archive Appliance
- Archive volume wrapping keys protect each archive volume's file level encryption keys
- All file level symmetric encryption keys are protected within a Dedicated Encryption Key DR Vault
- Dedicated Encryption Key DR Vault keys are never stored with the encrypted data files
- File level keys are always backed up and vaulted before being committed to use, ensuring retention of all encryption keys
- Master and archive volume encryption keys can be managed by multiple security officers

Transparent operations for users and applications

- User-based authentication and access controls - user or entity identification locks down data access.
- No operational changes are required for data access.
- Use of symmetric encryption keys eliminates the requirement for communication of public keys.
- Utilizes industry standard access control via Active Directory, LDAP, and Local Users for all access to data.

Secure Transmission of Data

- Data at rest is encrypted and protected at all times.
- All data is securely encrypted and transmitted during data replication via secure network communications protocol

Manufactured under ISO9001 registered quality system

Alliance Storage Technologies Inc.