

## SecureVTS Tape Encryption for Virtual TapeServer

### Highlights

- Protects data from unauthorized access
- Achieves regulatory compliance for virtual and physical tape
- Deploys on existing hardware platforms
- No impact to host server environment
- Leverages powerful 256 bit AES (Advanced Encryption Standard)
- Complete key life cycle management
- Seamless integration with VTS supported physical tapes and libraries
- Flexible – encrypt only the data needed, when needed

### Overview

The number of publicized security breaches over the past 2 years has been alarming, as have been the fines, penalties and legal burdens placed on companies. Minimizing data at rest risks, maintaining regulatory compliance and keeping out of headlines has become a priority for business leaders.

SecureVTS is a software module for the Virtual TapeServer (VTS) that encrypts and decrypts backup data being written from one or more host servers. Industry standard encryption algorithms and embedded key management are used to satisfy regulatory requirements and protect stored data from unauthorized data access.

Every enterprise defines different policies regarding backup, archive, and retention requirements. Storage Administrators and Security Officers will find it valuable to integrate VTS with SecureVTS to ensure selected data on disk as well as data written to physical tape are protected in the event of a security breach or the media becoming compromised.

### Key Benefits

#### *Strong Encryption*

The algorithm used by SecureVTS to encrypt data is the Advanced Encryption Standard (AES) with a 256-bit key length. Data compression and encryption are performed inline as data is written to the VTS disk system. During a scheduled migration of critical data off to physical tape media, the data remains encrypted thus ensuring that the tape media is securely transported off-site and archived in an unreadable form.

#### *Integrated Key Management*

Key management is a critical component to ensure encryption keys are safely handled. SecureVTS supports the complete key life cycle, ranging from random key generation, distribution, recovery & deletion of the encryption keys. The SecureVTS Key Server randomly generates a symmetric key for each file to be encrypted ensuring key randomness and preventing the reuse of keys.

The SecureVTS key management system consists of three components:

1. Data encryption using symmetric key encryption
2. Secure key storage by encrypting key database
3. Encrypted links between the encryption keys and the data

Users can be confident that data is safe since encrypted data is always separated from the keys stored in the embedded key database. Requests for keys must first be authenticated before access to keys is provided.

Keys are protected from loss by backing up the SecureVTS key database remotely and securely to another VTS or other system located offsite. For additional system redundancy, SecureVTS also supports clustering to allow the key database to be backed up locally to another node in the cluster.

## SecureVTS Features

### Ease of Use

SecureVTS uses a standard web browser connected to the VTS Management Interface and an intuitive, easy to use graphical interface to configure multiple role based access rights and user level privileges according to a company's security guidelines. SecureVTS requires an administrator role to configure system encryption functions. This prevents unauthorized persons from purposely or inadvertently modifying the configuration settings for data encryption.

### Flexibility

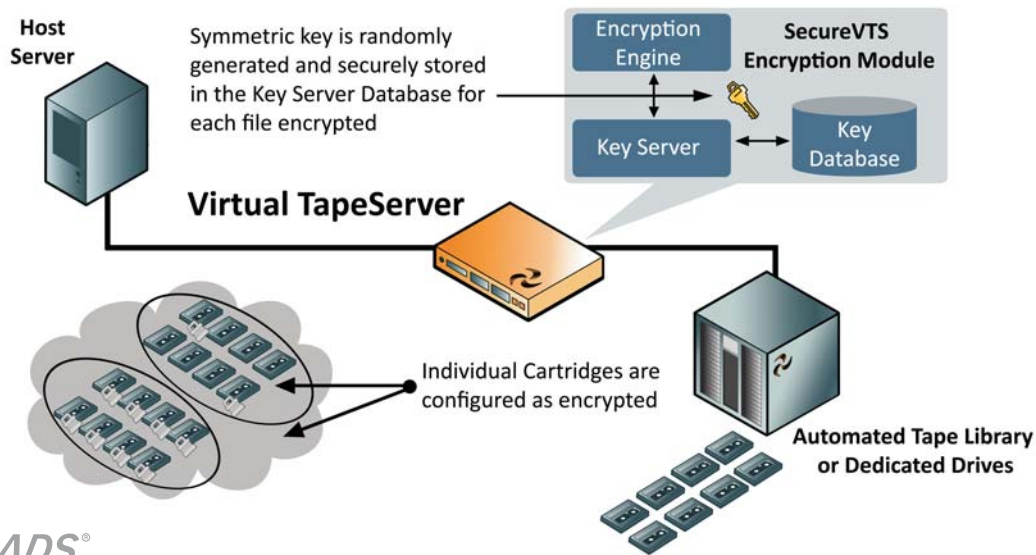
The flexibility of SecureVTS allows companies to tailor the solution to meet their specific needs. Critical data is selected for encryption during the creation of the virtual pool or cartridge by clicking a configuration setting from within the intuitive web based interface. Granularity at the virtual cartridge level ensures enterprises can encrypt critical data only when needed, thereby conserving valuable processing resources.

Encryption processing is performed inline as data is written to the VTS hard disk by first compressing files to remove repeatable patterns and then encrypting to hide recognizable patterns. The high-performance compression and encryption is transparent and automatic when the Virtual TapeServer pools or cartridge files are written to the VTS system.

### Interoperability

SecureVTS does not require any changes to host server environments or backup policies. Encryption processing and key management is transparent and other functions of VTS will operate normally.

SecureVTS interoperates with any VTS supported Host Operating System. In addition, secure migration of encrypted data to any connected physical tape drive or tape library can be scheduled normally using any integrated backup management application supported by VTS.



**Crossroads Systems, Inc.**  
11000 North MoPac Expressway  
Austin, Texas 78759  
USA

**TEL:** 866.BUY.CRDS  
866.289.2737  
512.349.0300

**FAX:** 512.349.0304

**EMAIL:** sales@crossroads.com

www.crossroads.com

**Crossroads Europe GmbH**  
Marie-Curie-Str. 19  
73529 Schwäbisch Gmünd  
Germany

**TEL:** +49 7171 99800-0  
+800 46243726

**FAX:** +49 7171 99800-10

**EMAIL:** contact-europe@crossroads.com

### ABOUT CROSSROADS

Headquartered in Austin, Texas, Crossroads Systems delivers flexible solutions to protect, secure and restore business-critical "data-at-rest." Crossroads (symbol: CRDS) is currently traded on Pink Sheets and also posts its financial disclosure reports, press releases and other related documentation on the OTCIQ web service of the Pink Sheets website. For more information, please visit [www.crossroads.com](http://www.crossroads.com).



Crossroads promotes institutional and personal environmental responsibility within the company, with our partners and with the users of our products. We are committed to providing the best products and services while encouraging practices consistent with sustainable living and resource conservation.