

WHITE PAPER

**THE BUSINESS CASE FOR  
A TAPE ENCRYPTION APPLIANCE**



## EXECUTIVE SUMMARY

Recent history has demonstrated that data stored on tape is vulnerable to unauthorized access and use. According to recent Enterprise Strategy Group estimates, more than 72% of all backed up enterprise data resides on storage media in unprotected plain text. Global enterprises such as Bank of America, Ameritrade, Time Warner, and Citigroup have all been recently victimized by tape theft and exposed to incalculable business risks. In all cases, the risks resulted from the tapes being physically unsecured, and once accessed, the data on the tape could be easily read.

To control these risks, companies must exercise greater diligence in protecting tapes, and ensure that data on tape cannot be utilized even if accessed illicitly. By encrypting data, companies can efficiently and cost effectively render data on the tapes unreadable to unauthorized persons.

## AGGRESSIVE DATA PROTECTION IS ESSENTIAL

Regardless of how corporate data is stored, it is clear that more secure methods for protecting data is required. First, increasing volumes of sensitive data are being stored by an increasing number of business applications, including backup, archive, and audit software. Second, increasing numbers of government regulations (SOX, HIPAA, PCI, Gramm-Leach-Bliley, etc.) mandate that the privacy of stored data be rigorously protected, with stiff monetary penalties stipulated for failure to do so. Third, legislation in 22 states calls for public disclosures of suspected breaches of consumer information, so a data loss can quickly lead to a loss of confidence—and of customers. And fourth, should business critical data fall into malicious hands, corporate viability can be threatened.

## TAPE IS HERE TO STAY

As a result of recent data breaches, government regulations, and overall data explosion in corporations, enterprises are confronted with a need to have an economical, long-term and scalable backup strategy. Tape has long been an ideal medium to meet these requirements because of its low cost, deep archiving, removable and readily available characteristics. According to Freeman Reports, the costs of tape storage per gigabyte are actually falling 45 percent each year. With more than 80 percent of all computer data already stored on tape, and 99.9 percent of all archived data stored on tape, it is clear that tape is here to stay.

Ironically, these issues, and associated risks, tend to be linked to one of the key benefits of tape—its portability. Easy to transfer from one site to another, tape is also easy to steal and misplace. And, with the ubiquity of standards-based tape drives, tapes are also easy for unauthorized users to read.

## ENCRYPTION: METHOD FOR PROTECTING DATA ON TAPE

Enterprises are facing new business pressures from highly, distributed work environments, intellectual property fluidity, increased data accountability and government regulations. This has forced companies to look beyond traditional perimeter-based security methods and evaluate alternative technologies to ensure data security and integrity. Datacentric measures, like data encryption, that protect the information directly, independently of the infrastructure components that store, transmit, or process data has gained industry acceptance and recognition. Data encryption has emerged as a powerful and effective way of protecting data-at-rest, especially in the storage organizations. Companies are increasingly implementing solutions that encrypt business critical data to ensure that even if someone has authorized access to the tape library, they do not, by default, also have access to the data on individual tapes.

### ALTERNATIVE APPROACHES FOR TAPE ENCRYPTION

Companies have 3 options to encrypt their tape backups. Data may be encrypted by the backup software, through specialized tape drives, or with a free-standing encryption appliance.

Although backup software is often touted as being the least costly and easiest way of encrypting data, it should be noted that these applications fall short in several critical areas that severely limit their utility as an effective encryption tool.

- **Limited Security** – relies on outdated encryption algorithms such as DES or triple DES, when newer, industry-standard algorithms such as AES- 256 are used for robust encryption. Moreover, encryption keys can often be easily compromised because they are generated by a pass phrase entered on the client, and stored in clear text.
- **Poor Performance** - software encryption and decryption are CPU-intensive tasks and limits throughput of backup and restore data streams. The software encryption imposes additional overhead on the backup client while it's backing up. Moreover encrypted data doesn't compress well, so any data compression will have to be done on the client, adding to the CPU overhead.
- **Weak Key Management** – lacks a centralized, scalable and secure key management system for large and distributed encryption environment. Offers limited capability with respect to key life-cycle management, ranging from key generation, distribution, sharing, to archiving, recovery & deletion.
- **Hidden Costs** – incur costs on buying additional physical tape media to store excess data as a result of not being able to compress data prior to encryption. Additionally, the throughput of the backup will be cut significantly and therefore the backup window will increase as a result. The only option to the customer will be to purchase more backup licenses and more physical devices to make up for the loss in performance.

As an alternative to backup software, data may, theoretically, be encrypted at the point of storage, on individual tape drives. Although this approach would certainly deliver improved performance as compared to backup applications, there are significant limitations.

- **Partial Support** – lacks support for a heterogeneous tape environment. These drive-based solutions come with the limitations of vendor specific environments and additional cost for the enhanced drives.
- **Limited Flexibility** – lacks software decryption tool that helps to recover encrypted data in wake of a disaster. Since the same manufacturer's drives and libraries must be used for both encrypting and decrypting data, end-user configuration flexibility—and access to low-cost, best-of-breed tape solutions— is severely limited.
- **Expensive Solution** - requires newer, high-cost, specialized drives and in a few cases a very expensive upgrade option is available. Moreover, because of a lack of support for heterogeneous tape environments, customers will not have the option to choose from low-cost, best-of-breed tape solutions.

### ENCRYPTION APPLIANCES: THE ULTIMATE TAPE PROTECTION SOLUTION

Hardware appliances are currently the most flexible, scalable, and cost-effective way of encrypting data because they act as a vendor-neutral front-end to the tape library, compressing and encrypting any or all data streams as required. With appliances, compression and encryption are core functionalities—not bolt on features as they are with backup software or tape drives and libraries.

By providing a single path to the tape devices for all data written to tape, appliances can optimize network bandwidth utilization, and enable data streams from multiple applications to be protected without impacting the performance of those applications. With an appliance, for example, the performance of backup software is never decreased when data is encrypted.

## THE BUSINESS CASE FOR A TAPE ENCRYPTION APPLIANCE

Furthermore, as data volumes requiring encryption increase, appliances can be easily scaled. Some appliances even support multiple ports and can process multiple data streams concurrently, to ensure the best possible throughput in high volume environments. Also, with an appliance, individual data streams can be variably encrypted and compressed, or simply passed through to a tape drive.

Another benefit of appliances is that they are vendor-neutral, able to seamlessly interface with virtually any disk drive, tape library, or software application that writes to tape. This can be a critical benefit because decryption of data encrypted with an appliance does not require a specific manufacturer's library or any additional software solutions.

Appliances also take advantage of the most robust encryption algorithms available—AES with 256 bit keys and cipher block chaining. With the single purpose of protecting data on tape, appliances offer the robust feature set required for this task, including a secure Web-based management interface with full SSL support and two-factor authentication. And, of paramount importance is the support an appliance provides for best-in-class encryption key management, with built-in quorum-based key recovery.

## ENCRYPTION APPLIANCES MAKE GOOD BUSINESS SENSE

Encryption appliances make the most business sense for companies seeking to protect their essential tape-based data resources because they can be seamlessly, quickly, and cost-effectively integrated within existing storage architectures. With a vendor-neutral encryption appliance, no software upgrades are required and legacy investments in tape hardware solutions can all be leveraged.

Encryption appliances also provide unmatched performance because of their ability to encrypt multiple data streams concurrently with no degradation in the performance of applications spooling data to tape, or of the tape drives themselves. The devices are also unique at this point in providing the most robust encryption key management capabilities.

Proper security for data storage is imperative to ensure data integrity as well as to mitigate the damage that compromised or stolen data can have on a company's long-term corporate image and financial standing. With tape remaining the medium of choice for low-cost backup and archival of data, the right encryption appliance ensures companies have an unprecedented degree of protection against inherent security risks of tape usage for backup and archival.

### ***About Crossroads Systems, Inc.***

Headquartered in Austin, Texas, Crossroads Systems is a global leading provider of data security, resiliency and connectivity solutions. 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 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](mailto:sales@crossroads.com)

[www.crossroads.com](http://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](mailto: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 webservice 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.

© 2008 Crossroads Systems, Inc. Crossroads and Crossroads Systems are registered trademarks of Crossroads Systems, Inc. Specifications may be subject to change.