

## Information on Backup Encryption Methods

### General Information on Backup Encryption Options

<http://www.csoonline.com/analyst/report3945.html>

### Examples of Removable Hard Drives from Dell

<http://search.dell.com/results.aspx?c=us&l=en&s=bsd&cat=prod&cs=04&k=encryption+tape&img=True&sum=True&ssum=False&qmp=12&p=1&eh=NoEvent&rrr=False&subcat=2999/5683&sort=K&snpsd=A&ddate=False&ddays=&nf=&dt=&navla=&fm=&ss=&ira=False&cp1=-1&cp2=-1&si=>

### Information and Links on Hardware Tape Encryption

[http://searchwincomputing.techtarget.com/tip/0,289483,sid68\\_gci1134728,00.html](http://searchwincomputing.techtarget.com/tip/0,289483,sid68_gci1134728,00.html)

### Review of Tape Encryption Drives

[http://www.byteandswitch.com/document.asp?doc\\_id=85609](http://www.byteandswitch.com/document.asp?doc_id=85609)

### Article on Encryption Tools

#### Tech Roundup: Tape/Disk Encryption Tools

By Stephen J. Bigelow, Features Writer  
16 Mar 2006 | SearchStorage.com

More than 50 million Americans have had their personal information compromised in the last year, and many of those security breaches have been the result of tape loss. With so much data at risk -- and the potential penalties involved -- storage administrators are struggling to protect sensitive information at rest in the data center and in flight across public networks. Vendors also see the problem, and are stepping forward with software and appliances that can ease implementation. The trick is to sort through the proliferation of offerings and find a product that meets your business requirements without breaking the budget. This article provides an overview of encryption and its role in the enterprise, highlights the leading vendors in the marketplace and offers some advice to help ease purchasing and implementation issues.

#### The reality of encryption

Simply stated, encryption is a technique used to make plain data unreadable. Encryption starts by processing data through a complex mathematical algorithm (a cipher) that uses a unique variable value (or key) to produce unique encryption results. Longer keys, used in concert with more complex encryption algorithms, will result in encrypted data that is practically impossible to recover without the key. Once the data is in an unreadable form, it is considered safe even if the files are lost or compromised by hackers. Encrypted data is made readable again (or decrypted) by processing it through the algorithm using the same key, though sometimes a different or companion key might be used for added security.

This simple concept has important implications for data center security. Given the growing number of high-profile security breaches in the news, storage professionals are embracing encryption technologies to protect the business against embarrassment and legal liability. "For the enterprise, encryption helps safeguard, protect and conceal data while it's at rest, being transported or being moved across networks," says Greg Schulz, founder and senior analyst at Storage IO. Encrypted data remains secure even when it is stolen -- a thief would need to have the encryption key or the computer processing resources available to "crack" the key by systematically attempting every possible key combination.

Analysts point out that encryption itself is not necessarily enough to mitigate corporate liability for lost or stolen data. "Does encryption let you off the hook totally? No," Schulz says. "Being able to demonstrate that you've taken some level of precaution (including encryption) does eliminate some liability." The underlying message is that encryption should be implemented to complement or expand the existing IT security strategy.

#### Considering encryption

An encryption strategy must start with a complete evaluation of corporate security vulnerabilities. In other words, you need to know what needs to be encrypted and at what points. Not all files must be encrypted, and encryption

may not be needed at every location in the enterprise. According to analysts, encryption is best suited for "at-risk" data that must leave the data center onto an unsecured network. "You should consider using it [encryption] when you have data that you believe could potentially be accessed by an unauthorized person," says W. Curtis Preston, vice president of data protection at GlassHouse Technologies. "I wouldn't use it where the cost significantly outweighs the risk."

Once you identify the data that needs encryption, it's important to define where the encryption will be implemented. Encryption can be used to protect data in flight across a network and at rest on a hard drive (or tape) in the data center. Protecting data in flight is particularly important when corporate data must be transmitted over open or unsecured networks such as the Internet. Protecting data at rest is a more recent consideration and is typically applied to tape backups that are sent off site. However, an increasing number of corporations will also opt to encrypt data on disk in the data center to guard against data loss from hackers or employee theft.

Although encryption works the same way on any target media (including hard drives, optical disc and tape), it's important to consider the implications of encryption on tape compression. "Encrypted data, by its nature, cannot be compressed," Preston says. For example, if you receive an average of 2:1 compression on a 10 gigabytes (GB) tape, you can fit up to 20 GB of data on the tape. If the data is encrypted first and is uncompressible, you'll need to use two 10 GB tapes -- doubling your tape media costs. To avoid this potential problem, implement encryption after compression.

Encryption is a mathematically intensive process, and can have a negative impact on the performance of your network depending on the type of encryption, the way it is implemented and the amount of files being protected. Strong encryption (such as AES 256) is more intensive than other weaker forms of encryption. More data takes more time to encrypt. And of course, software encryption products also take much more of a performance hit than hardware-based products. Analysts note that software encryption can impose a 40-50% performance hit on your network. By comparison, a hardware encryption box might only impair performance by 10% or less.

The trick is to find a product that meets your needs with a minimum performance penalty. For example, suppose you only need to encrypt a single database. A software encryption tool might only cost about \$500, while the extra few minutes needed to encrypt the database (and the extra storage space for that uncompressed file on tape) might barely be noticeable. When encrypting the entire data center, however, it probably makes more sense to use encryption hardware to minimize the performance penalty across a huge volume of data -- even though you will have to spend about \$30,000 per box.

Finally, any move to encryption must involve a close examination of key management. Lost keys can render corporate data inaccessible, so a potential adopter must learn how encryption keys are held or maintained and understand the risk involved. "The risk is that you lose your key," Preston says. "If you lose your key you've lost your own data." Key management policies and practices must be implemented along with any encryption technology.

### **Vendors and product selection**

There are essentially three means of encryption for the enterprise, and the choice of technology will largely dictate your vendor selection. The first approach is 'source encryption' -- encrypting data at its source directly through a particular application. Most operating system and application vendors (including Microsoft and Oracle) provide a means of data encryption. A second means of encryption is typically provided through backup software applications including EMC Corp.'s Legato, Symantec/Veritas NetBackup and IBM's Tivoli. The backup software can encrypt data on its way to tape. This enables the tape to be transported and stored securely off site.

The third avenue of encryption is a relatively new breed of dedicated encryption hardware devices from vendors including Decru Inc.'s DataFort security appliances, the StrongBox SecurDB from Crossroads Systems Inc., and the CryptoStor appliance family from NeoScale Systems Inc. Vendors like SpectraLogic also integrate encryption software functionality into their tape library products. Although hardware encryption is more expensive than software-based products, hardware offers superior performance and minimal impact on network operation. "The idea is they become an invisible piece of the infrastructure," Preston says. "All data going in and out of them is compressed and encrypted at line speed." Even hard drive manufacturers are adding encryption to some disks. For example, Seagate Technologies and Secude IT Security GmbH have joined to implement full disk encryption on the Seagate Momentus 5400 FDE notebook hard drive.

## **Selecting the right product**

Encryption success depends on an understanding of your security needs, then weighing the cost and performance tradeoffs of each product against those needs. While there is no single product or set of criteria to consider, analysts suggest the following points that can help you identify the best product for your own production environment.

Know the impact on performance. Every encryption product will have an impact on network performance. Software products will impact performance more than hardware products (but hardware costs significantly more). Understand how your choice of product and the volume of data being protected will influence network operation when encrypting data at rest and in flight. Know whether the product is optimized to encrypt at rest, in flight, or both.

Do not forego compression if possible. When encrypting to tape, find a product that allows for compression prior to encryption. Otherwise, compression to tape may be impossible, and tape costs will increase dramatically.

Have a clear picture of key management. Examine the product's key management system closely under primary onsite, remote (offsite) and DR scenarios. Determine how the system can fail or be defeated. In many cases, a multi-key system that involves several IT professionals is preferable to a single-key system left to one individual. Make sure that there are no 'back doors' that can be exploited. Understand how keys will be managed now and into the future.

Test products in advance. Bring products into the lab and test them in advance before making any purchase commitments. Testing ensures that products can actually deliver the performance and features that are expected, while interoperating with your existing infrastructure. This is also an ideal opportunity to evaluate the responsiveness and expertise of vendors.

Challenge product safeguards. Encryption is all about security, so test each product's safeguards against tampering. Encryption products with weak (or non-existent) safeguards should be avoided.

## **Best practices for implementation**

Once you've selected a new encryption product, storage administrators still face the challenges of installation and integration in the production environment. Although a vendor can provide support with product-specific guidelines, analysts offer some general policies that can help to streamline the implementation process.

Formalize key management procedures. Encryption keys are unquestionably the Achilles heel of any encryption strategy. An organization simply cannot afford to lose an encryption key, so an administrator must take steps to document the formal key management process and ensure that IT personnel adhere to the process. Documentation may need to be updated periodically as encryption targets change or new encryption standards are adopted.

Periodically test key management. Once established, key management practices should also be tested regularly to ensure that responsible individuals (key holders) each know their role in routine operations as well as disasters -- such drills will prevent confusion in critical crisis situations.

Balance security with productivity. When implementing a security product like encryption, it's important to protect only the data that requires protecting. Locking down every file with encryption can reduce network performance needlessly. In actual practice, only sensitive data needs to be encrypted -- and the strongest encryption may only be needed for the most sensitive data. Implement encryption so that it addresses business needs without bringing productivity to a standstill.