

QUICK TAKE



September 21, 2005

Your Best Tape Backup Encryption Options

by **Galen Schreck**

with Laura Koetzle and Sarah Bernhardt

EXECUTIVE SUMMARY

Following the highly publicized losses of backup tapes containing sensitive information about firms' customers, many organizations are examining their own policies and technology options for protecting data when it moves outside their corporate walls — such as backup tapes or tapes of customer information sent to business partners. Firms have three primary options for encrypting data before it goes out the door on tapes: 1) Turn on database encryption; 2) turn on tape backup encryption; or 3) install a storage encryption appliance.

Turning on encryption in existing database or tape backup tools will help firms close the security gap fastest for vulnerable servers. But firms with performance concerns, large volumes of encrypted data, and a healthy technology budget should consider specialized storage encryption appliances.

GOOD IDEA: ENCRYPT DATA USING DATABASE ENCRYPTION

Many databases like Oracle support table encryption as well as encryption specifically for backups. Database encryption will protect data on disk or on tape, and it's generally included with the core database features.

Pros:

- **Database encryption is getting easier to use.** The latest version of Oracle's database includes encryption for backups. Unlike column-level encryption that adds overhead to every transaction, the backup encryption only takes place when the system is scheduled to back itself up.
- **Only select administrators have access to sensitive data.** Because sensitive information is encrypted before it leaves the database, even server and storage administrators with root access can see only the encrypted bits. Access can be limited to a handful of trusted database administrators (DBAs) or security administrators.

Cons:

- **Encryption slows database performance.** The encryption and decryption of encrypted columns can add processor overhead to every transaction.
- **Database encryption can be difficult to configure on older systems.** For example, applications running on an Oracle database older than Oracle 10g R2 or on IBM DB2 have to call an API to decrypt data that is protected with column-level encryption.

- **Other data is still exposed.** Database encryption fixes just one, albeit large, collection of data. That leaves firms with a piecemeal approach to encrypting other data sources.

BETTER IDEA: TURN ON ENCRYPTION IN THE TAPE BACKUP APPLICATION

Many tape backup vendors have built encryption capabilities into products already installed in many data centers — it's just a matter of turning them on for server volumes that contain sensitive data. As with database encryption, there is additional overhead on the server, and key management is very basic.

Pros:

- **You may have already paid for encryption technology.** Tape backup tools like CA ARCserve, IBM Tivoli Storage Manager (TSM), and VERITAS NetBackup all support encryption — although their algorithms vary. VERITAS NetBackup offers the strongest algorithms, including 3DES, 128/256 AES, and Blowfish, while CA ARCserve and IBM TSM support 3DES.
- **Encryption processing is distributed across backup clients.** To keep encryption from slowing down the backup server itself, the backup agent on the target server handles the encryption operation. As a result, overhead is distributed, and data is encrypted over the network as well as on the tape.

Cons:

- **Not all tape backup agents support encryption.** Currently, HP Data Protector offers an encoding algorithm that obscures data from the casual snooper but lacks the security of true encryption because the encoding algorithm could be reverse-engineered. However, interested customers can use HP Data Protector's API to integrate with third-party cryptographic software. While the latest version of IBM TSM offers 3DES (equivalent to a 168-bit key), prior versions only supported the much less secure DES, which used a single 56-bit key. Lastly, EMC's current version of Legato Networker 7.2 does not support encryption, which will be added in its upcoming 7.3 version.
- **Weak key management may be problematic.** Because encryption takes place on the backup client, each client needs to have its own encryption key. None of the tape backup vendors currently offer a centralized key management system; instead, keys are generated by a pass phrase that is entered on the client. The pass phrase must be manually stored in a secure location so if the server is destroyed, its encrypted tapes can be restored onto a replacement.
- **Overhead can still be an issue for touchy servers.** Although encryption doesn't place additional load on the backup server, it can impose some additional overhead on the backup client while it's backing up. Lastly, encrypted data doesn't compress well, so any data

compression will have to be done on the client, adding to the CPU overhead. Encryption will increase data volume by only 5%-7%, but deactivating the now-superfluous hardware compression functions, such as those found on LTO-3 tape drives, will double their data throughput to nearly 500 GB/hour.

BEST IDEA: INSTALL AN ENCRYPTION APPLIANCE IN THE STORAGE NETWORK

The latest storage encryption method to emerge uses hardware-accelerated appliances that sit in the storage network. Available from vendors like Network Appliance, NeoScale, and Vormetric, SAN encryption appliances sit directly in the data path and encrypt data at wire speed, while the servers and storage are unaware of their presence. Optionally, administrators can install software agents on the servers to enforce data access down to the user level.

Pros:

- **Appliances offer top performance with no server overhead.** Because they implant their encryption routines in hardware, storage encryption appliances offer the fastest data encryption. And because they sit in the data path, storage encryption appliances operate at wire speed and offer a variety of clustering options.
- **Strong key management facilitates recovery.** The key management built into storage encryption appliances is the best of any alternative presented above. The appliances' secret keys can be stored on a group of smart cards that firms can distribute to selected corporate officers. The appliance can be configured to support quorum-based recovery — in other words, a (configurable) subset of the key cards can recover the key if an appliance is destroyed.
- **Appliances offer more capabilities than tape backup encryption.** Besides encrypting tape backups, encryption appliances can encrypt all data written to SAN-attached storage. Some vendors like Decru, which was recently acquired by NetApp, can also encrypt data written to NAS appliances through the use of a proxy.¹ Finally, encrypted data can be digitally shredded by destroying selected encryption keys. This capability allows firms to surgically delete data stored on off-site tapes until a service-provider can degauss or physically destroy them.

Cons:

- **The best encryption technology also costs more.** Unlike database or tape backup security that has probably already been paid for, storage encryption appliances start at about \$20,000. Plus, because the appliances are in the data path, many firms will want to cluster one or more for redundancy and high availability.

ENDNOTES

- ¹ Network Appliance (NetApp) announced in June 2005 that it planned to acquire storage encryption specialist Decru in a cash and stock deal worth \$272 million. Storage encryption appliances have been around for years, but customers were often limited to the most paranoid of organizations — in fact, Decru was partly funded by In-Q-Tel, the CIA's venture capital arm. Thanks to recent events like Citigroup's missing box of backup tapes full of customers' private information, firms have begun to re-examine their data security. Forrester expects the combined NetApp-Decru product set to result in useful products for data security and regulatory compliance. See the June 17, 2005, Quick Take "NetApp To Acquire Decru: Storage Encryption Goes Mainstream."