Encryption Made Easy

Introducing the first tape drive with “on-board” data encryption: TS1120
BY AARON DALTON

In the first years of the 21st century, companies know more than ever about their customers. This knowledge is gained through the collection and analysis of customer data, but it comes at a price: companies are now responsible for securing the privacy data of their customers’ personal information.

Companies not only have a potential moral responsibility to protect information pertaining to customers’ trust from unauthorized access—they may also have the legal responsibility. An increasing number of jurisdictions have passed or are considering adopting laws mandating that companies notify customers about the loss or theft of their personal data.

Growing Concern

Over the past year-and-a-half, the general atmosphere of concern centered around data security, as data stored on backup tapes led to IBM customers wishing to ensure the data on their tapes was properly protected at all times. In response, IBM formed a cross-disciplinary storage and software task force charged with helping clients protect their customer data.

In July 2005, IBM announced its intention to provide encryption in a storage device outside of the server. Now IBM fulfills that promise with the TS1120 drive, a device that offers the ability to encrypt data at the tape-drive level.

“From a customer perspective,” says Brad Johns, program director, IBM Storage software and tape marketing, “the primary purpose of the TS1120 is to help customers address government regulations and take advantage of the latest IBM tape technology that builds on proven technology that’s already been very successful.”
Before IBM introduced the TS1120 drive, there were two main ways to encrypt data: a hardware option and a software option. The software option had the advantage of being applicable on an enterprise-wide basis, but it was an intensive user of server resources. Also, the encryption keys needed to access protected data tended to reside on the server or application that performed the encryption rather than being available across multiple servers.

In contrast, the hardware approach relied on special-purpose appliances sitting on storage area networks (SANs). As data passed through these appliances, it was encrypted and sent out to a storage device. While these specialized-hardware pieces placed no demands on server resources, the approach only worked well in situations where minimal amounts of data were encrypted. The hardware option didn’t provide a comprehensive approach but instead focused on specific servers or specific applications.

Security Keys
When IBM turned its attention to developing a tape drive with encryption capabilities, it realized that the primary challenge wouldn’t be in designing the hardware but rather in the area of key management.

“We spent a lot of time creating a language and terminology around encryption that reduces complexities and provides a common language across all systems,” says Johns.

When data is encrypted with a particular key, the same key is needed to later access the data. A company may store numerous tape cartridges off-site for a long period of time and recall the tapes years later when access to that data was needed. If the key is lost, the data becomes inaccessible.

For these reasons, IBM determined the process of generating and storing encryption keys had to be extremely secure but accessible for people who deserved access. The company’s cross-disciplinary task force devoted much time and effort to devising a superior key-management system before settling on a solution widely used in data sharing across the Internet—public-key cryptography. This method of data encryption relies upon the use of a public key with a known algorithm to encrypt data that can then be opened with a private key that the recipient holds.

The result of IBM’s efforts is the TS1120 drive, the world’s first encrypting tape drive. Encryption is a standard feature on all new TS1120 model E05 drives and a chargeable upgrade feature on existing TS1120 drives.

What are the advantages of handling data encryption of tapes within the tape drive itself? Handling encryption inside the tape drive avoids use of host resources. Performing encryption with the TS1120 drive causes less than a 1 percent degradation in tape-drive performance. Since tape drives are already part of existing storage and backup infrastructure, using the drive itself to perform encryption has a clear cost advantage over buying and installing a dedicated piece of hardware just to encrypt data. Essentially, the TS1120 drive offers a lower cost, high-performance way of getting the encryption job done.

Furthermore, the Java™ technology-based software used with the TS1120 drive is compatible with a variety of platforms. Companies can integrate TS1120 drives into their existing tape systems and libraries. The TS1120 drive is designed to operate smoothly and seamlessly with IBM System p™ hardware.

Recognizing that every company has its own data-security needs and organizational preferences, IBM has designed the TS1120 drive to be flexible in the way that it allows encryption-key management. There are three key-management options: system managed, library managed or application managed.

Choosing to manage encryption keys at the system level allows an organization to take advantage of key management tools built into the System p platform. From this central viewpoint, a storage administrator can specify that data from certain servers will be encrypted while data from others won’t. The option of managing at the tape-library level lets an organization choose not only which drives but also which tape cartridges should have their data encrypted.

Finally, the application-managed option gives a company’s existing storage applications the responsibility of generating and storing encryption keys. IBM has built the TS1120 tape drive to accept keys from applications such as Tivoli® software. In this case, Tivoli would perform the actual key generation, bypassing the use of TS1120 drive’s key-management software.

“From a customer perspective, the primary purpose of the TS1120 is to help customers address government regulations and take advantage of the latest IBM tape technology that builds on proven technology that’s already been very successful.”

—Brad Johns, program director, IBM Storage software and tape marketing
The Tivoli Angle
Tivoli is the first to explicitly take advantage of TS1120 drive’s capabilities with a complete encryption solution. Many Tivoli users work in an open-system environment, using software solely to back up, restore and archive their data.

Tivoli already offers data-encryption capabilities within its software, and Tivoli users who own a TS1120 drive can choose to continue performing small amounts of data encryption within the software without adversely affecting server performance. For larger data-encryption tasks wherein software encryption could have an adverse effect on network performance, the TS1120 drive can step into the breach, and encryption can be performed in the drive itself. In either case, a customer who has chosen the application-managed option can continue to use Tivoli’s key-management software, and existing disaster-recovery (D/R) process that tapes that go off site are encrypted.

Where Tivoli previously left key management to the user, the latest version of Tivoli Storage Manager (TSM) 5.3 assumes key-management responsibilities. TSM handles the key management by generating a key, passing it to the TS1120 device driver and telling the tape drive to use the key to encrypt a batch of data. TSM then stores that key alongside the metadata for the tape volume. The keys actually travel along with the other metadata in an encrypted format. Losing a key is practically impossible, since the keys don’t exist separately from the metadata.

Tivoli’s engineers have worked closely with IBM System Storage™ to help ensure the TSM 5.3 and the TS1120 drive work together to create a flexible system that allows users to decide which data should be encrypted and which keys TSM should manage. Since encryption can be directed at the cartridge level, organizations can specify that only those tapes traveling outside their premises receive encryption coding. And, of course, the tape encryption occurring within the hardware itself reduces overhead demands on the client’s network. According to initial feedback from early adopters, combining TS1120 drives with Tivoli software may improve client-server performance and create a faster, more secure system to manage and encrypt customer data.

The TS1120 drive may be a new drive with new encryption functionality, but it rests on a solid foundation of proven and reliable technology.

Tape encryption is too important a task to be postponed. There’s pressure to quickly implement a tape-encryption system with its attendant key-management protocol. To assist clients with tight deadlines, IBM has created a services team that can help companies rapidly implement TS1120 drives and develop a key-management protocol.

Of course, the TS1120 drives offer more than just encryption capabilities. The device still performs its primary function as a drive with world-class specs—data transfer rates up to 200 MBps with 2-to-1 compression, 400 MBps burst data rate and the ability to handle various media, including long- and short-length cartridges in rewritable and write once read many (WORM) formats. If the need does arise, the TS1120 drive offers 256-bit Advanced Encryption Standard (AES) security on demand.

Competitive Advantage
With the advantages in speed, oversight, security and efficiency that encryption-capable tape drives bring, it’s likely the TS1120 drive is just at the leading edge of what will grow into a larger trend. In five years, tape drives with built-in encryption capabilities may be ubiquitous at the high-end of the tape drive market—as common as WiFi in a notebook PC. Once companies realize how cost-effective and sensible it is to build encryption into tape drives, the demand for such products could skyrocket.

Someday, other drives may reach the market to satiate that demand, but for now, only the TS1120 drive offers this encryption functionality.

Privacy worries aren’t about to go away anytime soon—in fact, they’re likely to only become more intense. Even now, the banking industry is looking to create its own standards on data security that would reinforce government requirements. Missing the boat on tape encryption can expose a company not only to scandal, but, even worse, to a loss of trust among its customers that can be very difficult to repair. The organizational and capital efficiencies enabled by the TS1120 drive makes data-tape encryption not just a smart move but also a competitive advantage.

Aaron Dalton is a writer who specializes in business and technology topics. Aaron can be reached at aaron@imaginationwins.com.