



Strategies for Simplifying the Migration to Encrypting Tape Drives



Table of Contents

Executive Overview	3
The Move to Encrypted Tape	3
Drive-Based Encryption: Ready for Deployment?	3
Limitations in Migrating to Next-Generation Technology	4
Ensuring Recoverability of Backups and Archived Data	5
Solution: Intelligent Key Management for Multiple Points of Encryption	5
Comprehensive, Centralized Key Management	5
Transparent Encryption for Existing Devices	6
Migration Process	7
CipherMax Secure Enterprise Storage Security Enterprise	7
Support for Phased Migration	7
CipherMax Benefits	9
Summary	9

Executive Overview

As external and internal forces drive the move to secure tape-based data storage through the application of data encryption, next-generation tape drives with integrated encryption processing are coming on the market with the promise of low-cost, transparent security—solutions that effectively make software- and appliance-based point solutions for encryption no longer viable. In the near term, however, the high cost of migrating capital equipment and existing tape inventories rule out a forklift upgrade for most IT organizations.

Enabling a gradual migration from legacy tape devices to encrypting drives, libraries and media has two essential requirements: one is a secure, comprehensive key management facility that can enable the encryption functionality in new drives from multiple vendors, as well as support external storage security systems that provide encryption services for legacy equipment and media. The second is an external storage security system to encrypt data volumes using existing tape storage devices. Management of such data can also be dramatically simplified with the deployment of advanced key management features that automate the detection of drive generation, tape media generation, and data format, and apply the correct security policy accordingly.

CipherMax offers solutions that enable an affordable migration strategy from legacy tape drives to secure encrypting tape drives with minimal administrative overhead and interruption to backup operations.

The Move to Encrypted Tape

In response to the increasing number of regulatory and industry requirements for enforcing personal information privacy, partner data confidentiality, and financial reporting data controls, many organizations have identified tape-based media as the first target for securing their sensitive stored data. However, some enterprises have either been postponing the deployment of encryption or using a limited number of in-line encryption appliances as a stopgap measure in anticipation of next-generation tape drives that integrate encryption processing into the drive. These next-generation drives offer the promise of transparent operation, simplified management and significantly reduced cost by eliminating the need for add-on point solutions to provide encryption services.

Yet, native drive-based encryption will have its limitations for some time to come. These include constraints in the choice of tape drive/library vendors and models; the limited availability of enterprise-class, centralized key management applications; the need to replace existing tape cartridge inventories to support encryption; the need to migrate tape cartridge inventories to next-generation media that supports the encryption functionality; and the potential for disruption to existing data protection processes and operations resulting from the mixing of ciphertext (encrypted) with cleartext backup data. As a result, the migration from legacy tape devices to encryption-enabled ones will likely require additional processes and procedures to identify the most sensitive data, where and how existing media will be utilized, and how data is recovered where it is needed. For those organizations committed to the adoption of drive-based encryption, the complexities can be greatly reduced with the combination of careful planning, a transparent encryption facility for legacy drives, and the use of a common, centralized key management facility for all data-at-rest encryption needs.

Drive-Based Encryption: Ready for Deployment?

While encryption has been a long-anticipated feature in next-generation tape drive designs, only a limited number of solutions have been brought to market to date. At the high end, IBM's TS1120 and Sun Microsystems' T10000 drives start at over \$30,000 per drive, putting them effectively out of reach for most users. The latest generation LTO-4 drive technology provides a more cost-effective option for encrypting tape-based storage media, with integrated

encryption processing at price points ranging from under \$6,000 for SCSI drives up to \$12,000 for Fibre Channel-attached drives. However, not all of the currently available offerings offer a key management facility to handle the key generation, storage, loading, archiving and recovery processes. Neither do backup applications provide support for LTO-4 key management functions required to activate the encryption and manage the encryption keys.

Limitations in Migrating to Next-Generation Technology

Once their vendor, equipment and applications are selected, customers desiring to move to encrypting tape drives continue to be challenged with managing their backup process in an environment that supports multiple vendors, models and generations of tape drive technology. Few medium- to large-sized organizations have the resources available to swap out their entire tape infrastructure, including drives, libraries and up to tens of thousands of legacy tape cartridges stored in local and offsite facilities without exceeding their budgets or severely disrupting operations. Instead, the migration to next-generation technology is expected to take several years. In addition to budget constraints that prevent an extensive replacement of older technology, other migration factors include:

Lease term commitments – Enterprises that lease their equipment in three-year cycles plan to make capital investments incrementally, rather than all at once. CFOs are unlikely to accept expensive early lease terminations for a feature update, so the migration must take place over time. Hence, a bridging technology is needed to support the migration of legacy equipment that still has many years of its useful life remaining to an encrypting infrastructure.

Older tape library models – Next-generation drive technology may require newer tape libraries to support the latest features. Unlike tape drives that often require replacement after 3-4 years of use, tape libraries often have a longer life cycle, typically ranging from 7-10 years or longer. Libraries that are not forward compatible with the latest feature sets may not support the use of the newer encryption-enabled tape drives.

Tape cartridge inventory – Many enterprises have an inventory of several thousand tape cartridges with a valuation in the millions of dollars that have limited functionality in the latest tape drives. LTO-4 drives, for example, are read/write compatible with LTO-3 tape media in unencrypted format only, and only provide read support for LTO-2 media—limitations that effectively eliminate these legacy cartridges from rotation into scratch tape pools. Half-inch tape drive requirements are even more demanding, with the IBM TS1120 supporting only 3592 media and the Sun T10000 requiring use of the newest tape media technology specifically designed for use with that drive.

Data protection (backup) operations – Key management mechanisms currently provided with the introduction of encrypting tape drives and libraries have the potential to impact existing data protection (backup) processes and procedures. The use of ‘set and forget’ encryption key policies for tape drives that cannot support the ability to adjust for appending or overwriting existing tapes with the proper encryption key generally requires the creation of special tape pools for encrypted media and drives. The result is that new encrypting tape inventory must be held and managed separately from existing plaintext tape inventory. Tape infrastructures shared between business units having different security and encryption needs (including different encryption keys) require another layer of processes and procedures to manually manage the data encryption aspects of the data protection environment.

In the short term, these limitations require the tactical deployment of encryption technology that only protects specific, identifiable data or tape drives. The danger of pursuing this strategy is that sensitive stored data that has been overlooked or backed up to remote locations remains unprotected and vulnerable to loss or theft. By implementing comprehensive encryption that protects all backup data, the risk of exposure is significantly mitigated. In

addition, the use of encryption means that lost or stolen tapes are not subject to personal data breach disclosure laws and need not be publicly reported.

Ensuring Recoverability of Backups and Archived Data

Complexities in a phased migration to encrypting drives may also be introduced when trying to recover data on a different system from the one on which it was created. This may be the case where the required model of encrypting drive is not immediately available to decrypt the media, or where key sharing has not been enabled at the recovery location. Sharing data among partners via tape media, for example, requires some method of providing the partners with keys and a recovery device to access the data.

Meeting these challenges to provide a seamless, gradual migration from cleartext to ciphertext storage of tape-based backup and archive data is possible. By deploying the right combination of encryption and key management technologies, users can start with comprehensive encryption for both legacy media as well as native encrypting drives. Over time, users can migrate to an environment that includes all encrypting drives from one or more vendors, or to a mixed environment as desired.

Solution: Intelligent Key Management for Multiple Points of Encryption

Since a one-step conversion to a fully encrypted tape environment is not an option for most IT organizations, a phased approach provides a means of migrating over time in a cost effective manner. A strategy is required that accommodates business-level security policy requirements as well as capital investment and operating budgets.

Enabling a gradual migration from legacy tape devices to encrypting drives, libraries and media requires two core capabilities:

- 1) A secure, comprehensive key management facility that can enable the encryption functionality in new encrypting drives from multiple vendors, as well as support external storage security systems that provide encryption services for legacy tape drives, libraries and media. This key management system should be administered through a central interface that can provide services for all encrypting devices attached to the SAN.
- 2) An external storage security system that can cost-effectively encrypt data volumes using existing tape storage devices. The system should be transparent to hosts, data protection applications, SAN infrastructure (i.e., switches), drives and libraries, and support essential tape security features like data compression, integrity checking and tape media ID tracking.

Comprehensive, Centralized Key Management

A common key life cycle management system that uses a single interface to enable the use of encrypting tape drives and support external data encryption systems for legacy drives allows the enterprise to secure its backup and archival data while minimizing the complexity of managing multiple systems. This is particularly critical for heterogeneous environments, since the use of multiple proprietary key management systems could result in a confusing key management environment.

Key Management for Encrypting Drives – Addressing the key management requirements of LTO-4 drives requires a storage security system with the capability of loading encryption keys into the drive dynamically in accordance with pre-defined security policies. This ability to assign keys to drives and track their usage allows the security administrator to create one or more keys within a secure, physically separate facility and load it onto the encrypting drive for use without having to transfer keys using an external token or expose the keys in cleartext form. The newly created keys also need to be catalogued by tape drive assignment and media

label IDs of the cartridges used for storing data; archived; and eventually deleted, if required, based on business-level security policies for encryption key management.

Key Management for External Encryption Systems – In addition to supporting new encrypting drives, a central key life cycle management system should also support any encryption systems used to secure data recorded onto legacy tape drives. The same database can be used for all encryption systems within the SAN by capturing and recording the same data for the external encryption devices as from the encrypting tape drives. This includes tape drive to encryption key mappings using the tape media label IDs (also known as barcodes or volume serial numbers) to identify cartridges. These mappings provide a view of the user’s tape inventory and should include information on the encryption state, key application date, and last access date for each tape.

Transparent Encryption for Existing Devices

Since capital expense and operating budgets seldom allow for a complete upgrade across the data center for all tape drives and their legacy media, a device that can support cost-effective encryption for existing devices is the other essential component needed to support the migration process. To provide cost-effective services, the device needs to serve multiple tape drives, necessitating high connectivity and encrypted data throughput rates. The device must also be interoperable with different drive types found in heterogeneous tape environments.

Management of Existing Data – In addition to the cost of new equipment and media, there is the cost of converting stored data volumes from cleartext to ciphertext form. While those that opt to migrate their data as cartridges are recycled in scratch pools may not need this, for others, having their data stored at remote locations in cleartext form is a vulnerability carrying significant risk. Providing read/write intelligence that allows drives to detect the type of cartridge, whether it has previously been written in cleartext or ciphertext, and, if ciphertext, what key should be used, greatly facilitates the process of migrating data while supporting ongoing operational requirements.

Additional features that significantly ease the complexity of migration from an existing infrastructure and managing multiple keys include:

- Tracking individual tape cartridges by their unique media label ID (barcode or volume serial number). This feature is required to provide data restoration using a tape drive that may have been assigned a different key for encrypting its own tapes. Cataloging the media IDs and their associated keys within a database allows the appropriate key to be identified and loaded into the tape drive.
- Detecting whether data has been written in cleartext or ciphertext and apply the proper mode for reading the tape. This capability is essential for recovering data on legacy media that was originally written in cleartext.
- Maintaining volume headers in cleartext allows data backup applications to correctly identify tapes even if the encryption keys for that tape are not available. This capability is required to ensure previously encrypted tapes can be recycled to scratch pools, or to prevent these applications from parking tapes as “foreign” or “unidentifiable.”
- The ability to specify writing to previously encrypted media using a new encryption key. This capability facilitates the enforcement of key rotation policies from media in the tape scratch pool that require the application of new keys. Without this capability, the tape would retain its existing key, which might be expired or compromised, or require a complete erasure before allowing the application of the correct key.
- The ability to detect the type of media inserted into an LTO-4 drive and assign the proper mechanism for decryption. LTO-3 tapes that were encrypted using an external storage

security device should be identified as such, allowing an external device to decipher the data, rather than failing the restore job with an “Unknown Media Format” message.

Migration Process

A manageable and affordable migration process can be achieved with a three-step process when moving to encrypting tape drives:

1. **Enable use of new encrypting drives while providing encryption for legacy drives.** The encrypting drives may be deployed as part of the normal equipment upgrade cycle. Comprehensive security can still be achieved by utilizing an external system that can both address the encryption requirements of legacy tape drives and provide key management services for the new encrypting drives.
2. **Migrate tape storage over time to a common platform, if desired, with the gradual purchase of new equipment and media.** Encrypted legacy media can either be supported using the external encryption system together with older drive models retained for recovery purposes, or using new drives that detect the media type and hand off the decryption to an external encryption system for recovery.
3. **Over time, the user may desire to move to a key management system provided by the tape vendor.** Standards-based key management is still some time away, however, so it is unlikely that we will see vendors supporting key exchange and media decryption on each other’s tape drives in the near term, even where they both use a common tape standard such as LTO-4. Therefore, consideration must be made in multi-vendor environments how recovery will take place to ensure the proper equipment is available.

CipherMax Secure Enterprise Storage Security Enterprise

CipherMax’s CM140T storage security system meets the requirements outlined above for facilitating the migration to an encrypting tape drive environment. As an external encryption system for tape, the CM140T provides data security for backups made with non-encrypting tape drives. The CM140T also offers the unique capability of serving as a key management gateway to enable encryption functionality on LTO-4 drives and provide common secure key management services for both non-encrypting and encrypting tape drives.

Support for Phased Migration

CipherMax’s ability to support both legacy non-encrypting and next-generation encrypting tape drives allows it to enable a phased migration strategy as outlined in the previous section. A single unit or cluster of units can function as a key management gateway for up to eight LTO-4 drives, or provide a combination of support for LTO-4 drives and non-encrypting tape drives. The graphic below provides an example of a Phase 1 tape SAN with a mix of new and legacy storage devices.

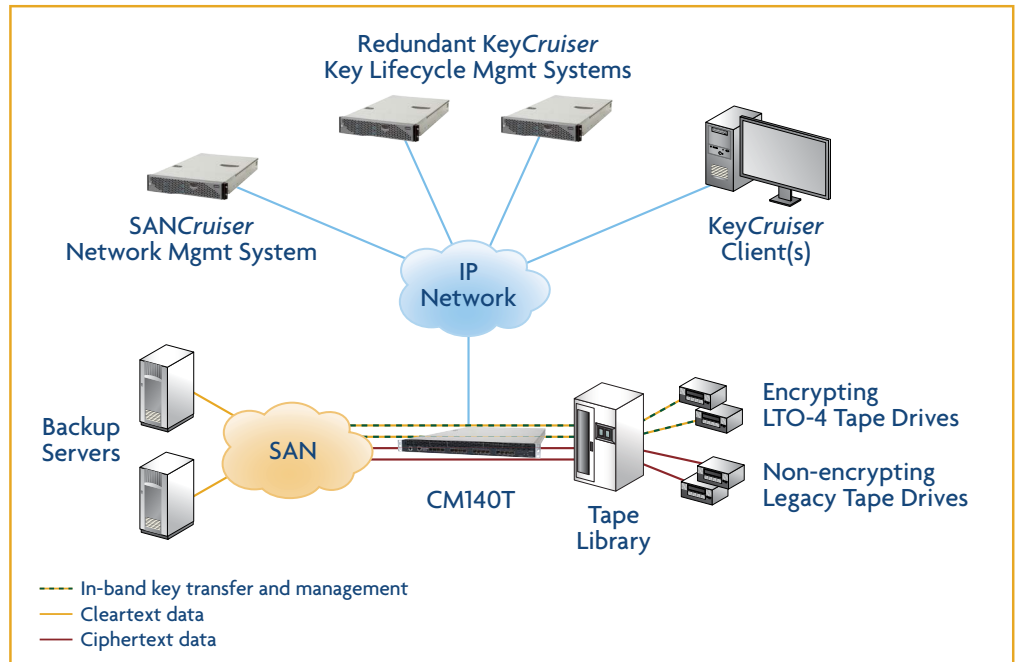


Figure 1: Key Management Support for Encrypting and Non-Encrypting Drives with Encryption for Non-Encrypting Drives

More encrypting drives can be added into the tape drive pool, permitting the gradual migration over time. As LTO-2 or LTO-3 drives are retired, users can still continue to read LTO-2 cartridges and read/write to LTO-3 cartridges in cleartext while using the CM140T for encryption and compression until LTO-4 media has replaced it entirely.

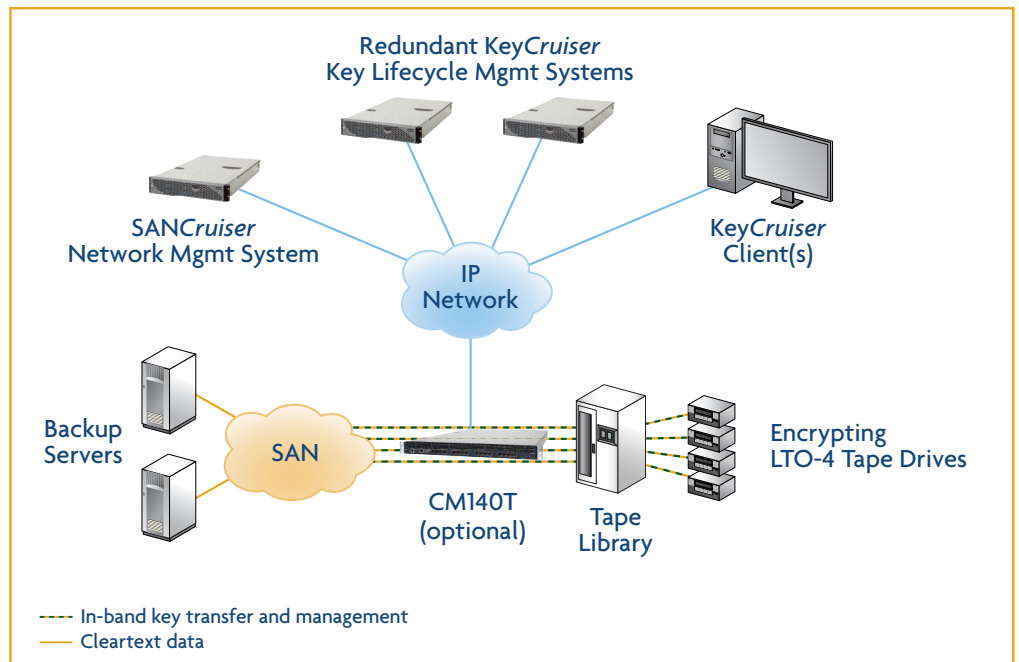


Figure 2: Key Management Support for Encrypting Drives and Decryption for Legacy Tape Media

CipherMax's advanced key management features give CM140T systems the ability to detect tape status and catalogue keys, providing security administrators with a high degree of control over their system key management. Advanced key management features include:

- Tracking individual tape cartridges by their unique media label ID
- Automatic mode detection of data (cleartext or ciphertext)
- Cleartext volume header that enables applications to identify tape volumes
- The ability to automatically apply new encryption keys to previously encrypted media
- The ability to automatically detect LTO-3 media in an LTO-4 drive and enable the use of the CM140T for cryptographic processing

This high degree of intelligence ensures the ability to manage keys over time, match keys to their respective media at any point in time, and ensure the recoverability of valuable data.

CipherMax Benefits

- Single, integrated system for LTO-4 key management and legacy tape encryption reduces cost by enabling a gradual migration strategy to next-generation tape drives
- Intelligent detection of tape status, mode and volume information reduces the complexity of key management
- Advanced key cataloguing and management ensures data recoverability at all times
- Single-pane-of-glass management for system administration and key management reduces administrative resources required to support a secure storage environment
- Ability to read encrypted legacy media using LTO-4 drives eliminates the need for expensive, time-consuming tape migration projects
- Complete feature set that enhances system auditability and minimizes operational costs.

Summary

While encrypting tape drive technology holds great promise for simplifying the process and management of backup data security, the initial adoption is likely to provide some unanticipated challenges and expenses. In addition to the cost of tape drives, upgrades to libraries and media need to be considered and expected, as well as tape cartridge management challenges in dealing with legacy unencrypted and encrypted media.

The complexity and expense of these challenges can be mitigated with a migration strategy that includes the use of an external system for enabling encryption in both new tape drives and legacy tape drives, and a comprehensive key management system that provides a common point of management and repository for all encryption systems.

For more information on CipherMax storage security solutions, please contact us at sales@ciphermaxinc.com or (408) 382-6500, or visit us at www.ciphermaxinc.com.

CORPORATE HEADQUARTERS

CipherMax, Inc.
1975 Concourse Drive
San Jose, CA 95131 USA
Tel: +1-408-382-6500
Fax: +1-408-382-6599

CIPHERMAX ASIA-PACIFIC

CipherMax, Inc.
Room 1035
Shanghai Central Plaza
381 Huai Hai Zhong Lu
Shanghai, 200020
Tel: +86-13601216832

CIPHERMAX EUROPE

Accentuate, Ltd.
Inglewood
16 Harebell Hill
Cobham, Surrey, KT11 2RS
United Kingdom
Tel: +44 (0) 7768 340498

ADDITIONAL CONTACTS

General: info@ciphermaxinc.com
Partners: partners@ciphermaxinc.com
Marketing:
marketing@ciphermaxinc.com
Sales: sales@ciphermaxinc.com
Technical Support: 1-800-670-4423

WEBSITE

www.ciphermaxinc.com