

Solution Overview: SecureVTL™

The CipherMax enterprise class storage security system for tape combined with VTL based storage creates a secure VTL solution that addresses the security requirements of industries like retail, financial services, healthcare and public corporations that are impacted by data confidentiality and control mandates, or have requirements to protect their intellectual property. SecureVTL adds a transparent layer of security to VTL-based storage that addresses these issues and prevents data access and viewing by unauthorized users. The Secure VTL solution provides:

- Transparent security with strong encryption for VTL-based data
- Protection for replicated VTL data and data exported to physical tape media
- Integrity verification for archived data
- Convenient, single pane of glass management for enterprise environments

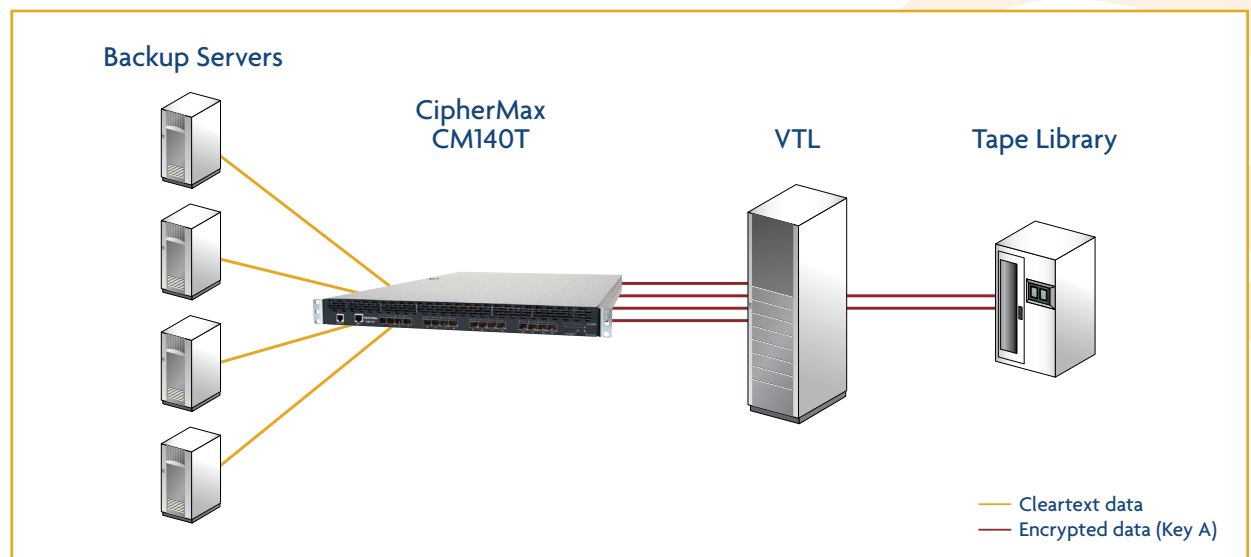
Why SecureVTL?

The increased popularity of disk-based backup solutions like Virtual Tape Libraries (VTL) has resulted in the

introduction of new risks into the storage environment. Examples include the ability for rogue insiders to connect unauthorized hosts to VTL servers to gain fast access to backup data, the increased concentration of data on a single storage system that could potentially be exposed, the reliance on low-cost SATA drives that are more prone to false positive failures resulting in RMA exchanges with exposure of data, and the increasingly common use of remote data sites for replicated data outside the confines of the data center security perimeter. By transparently layering in a suite of security technologies, including data-at-rest encryption, storage access control, integrity validation, and secure system access auditing to the VTL solution, organizations can ensure that their backup storage meets and exceeds the required standards for data privacy and security.

What does the SecureVTL solution include?

SecureVTL adds a CipherMax CM140T for Tape system to the VTL system. In addition to the fabric-attached CM140T device, the CipherMax system includes the *SANcruiser* Network Security Management and the *Keycruiser* Key Lifecycle Management applications.



How does the CM140T install?

The CM140T installs between the backup server and VTL system. Data written to the VTL disk as virtual tape backup is first compressed and then encrypted using an IEEE standard AES-256 algorithm. The disk-based storage is handled just as it would be to a physical tape backup, allowing seamless exports of virtual tape to physical tape of secure data. The CM140T also provides a data integrity check feature that confirms data has not been tampered or corrupted while in archival storage.

The CM140T can be configured as transparent to the SAN in Controller Mode, trunked to an existing SAN fabric in Discovery Mode, or as the SAN fabric itself in Switching Mode. The CM140T's flexible installation options ensure compatibility and easy installation and configuration.

How can the SecureVTL solution protect my replicate backup data?

The CM140T is configured such that backup data to the primary VTL system is already encrypted before the replication process occurs. As virtual tape is replicated, the data remains encrypted, securing both "data in flight" on the wire and "data at rest" at the remote facility, whether on disk-based virtual tape or exported to physical tape media. By deploying a CM140T at the remote facility

and establishing a trust relationship with the KeyCruiser, data can be recovered remotely in case of a catastrophic event.

What is the impact on backup operations?

The CM140T high port count connectivity with line-speed throughput and optional deployment configurations ensure completely transparent operation with respect to performance, interoperability and backup processes. Hardware acceleration for both compression and encryption processing supports backup rates at speeds equivalent to six LTO-3 tape drives.

How do I manage the encryption keys?

CipherMax's KeyCruiser features a Tape Media—Key Mapping Database that maintains an association between an encryption key and its corresponding tape backups, whether virtual or physical. Data can always be recovered from either virtual or physical tape as long as a CM140T device or the CipherMax Data Recovery Utility software is available. KeyCruisers can be clustered for high availability and reliability.

Where can I get more information on the SecureVTL solution?

For more information, please contact CipherMax at sales@ciphermaxinc.com or call 408-382-6500.

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

ADDITIONAL CONTACTS

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

WEBSITE

www.ciphermaxinc.com

