

KeyCruiser™

Advanced Key Lifecycle Management System for Assured Data and Recoverability

KEY BENEFITS

Global key facility for all CipherMax devices simplifies key management

LTO-4 drive support enables migration to integrated encryption technology

Advanced key management features minimize impact to operational workflows

Automated backup of all keys and configurations ensures data recoverability

Clustered architecture provides high system reliability

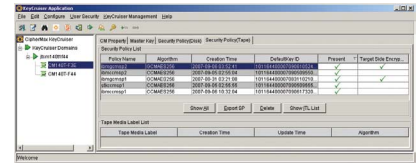
Overview

Modern encryption technology depends on the safekeeping of digital keys to enforce the confidentiality of valuable data, and the availability of those keys to decipher scrambled data back into useful cleartext. Insecure methods of key archival, distribution, recovery and destruction that do not promote reliable protection processes put both the security and the recoverability of the data at risk. Simplifying those processes with automation and global administration makes data security cost-effective and reliable to implement and manage.

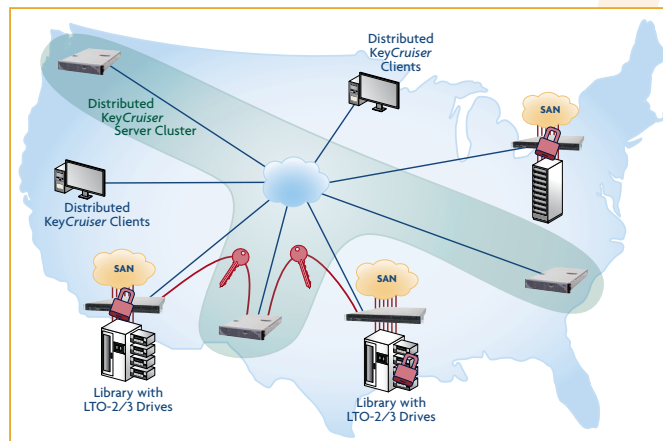
KeyCruiser is an advanced key lifecycle management system that ensures the recoverability and confidentiality of data protected by CipherMax storage security systems. KeyCruiser serves as a nearline, automated storage facility for the entire encryption key database, providing access to hundreds of thousands of digital keys that CipherMax systems use to encrypt sensitive stored data. KeyCruiser also protects every security policy and system configuration parameter needed to perform a partial or complete CipherMax system recovery and ensures that keys are secured throughout their lifecycle — readily available to trusted users for data recovery.

Secure Key Repository

CipherMax's CM systems have the capacity to store thousands of keys used for day-to-day access. KeyCruiser-managed keys are automatically archived for their protection across a secure link to a central key database. KeyCruiser receives and stores keys in a multi-layered, highly secure format, allowing keys to be safely stored outside of the CM system and ensuring confidentiality of data at all times.



As the central key repository for CipherMax operations, KeyCruiser is able to support widespread, distributed storage operations as required for both disk and tape encryption. KeyCruiser also provides for the recovery of data from remote locations when requested by trusted CM systems. A single KeyCruiser cluster can easily scale to support the demanding requirements of large enterprise environments, supporting deployment in multiple distributed locations and mitigating the potentially disastrous impact of a regional catastrophic event.

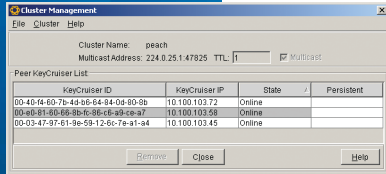


Painless Migration to LTO-4 Encryption

LTO-4 drives with integrated encryption processing offer the promise of convenient and cost effective security services for tape-based backup data. Like alternative encryption solutions, however, they require sophisticated key management support to

implement these services with minimal disruption to backup operations and workflow.

KeyCruiser not only supports data encryption using legacy tape drives like LTO and DLT, but also supports key management for LTO-4 drives with integrated encryption processing.



Users can set and manage security policies from a global interface for their entire storage environment with secure protection by *KeyCruiser* for later retrieval.

Advanced Key Management Functions

CipherMax's advanced key management features facilitate the migration from cleartext to ciphertext data storage. By automatically applying security policies based on tape and drive status detection, media containing cleartext or ciphertext data are handled consistently during backup operations. This ensures the application of the appropriate cryptographic process and key. Organizations with key rotation policies can easily recycle tapes containing ciphertext by designating the application of a new key. Business-level security policies defining the application of encryption are automatically enforced for CM-encrypted as well as LTO-4 drive encrypted data.

Managing Multi-Generation Tape Pools

Managing multiple generations of tape media to enable the use of encrypting drives can also introduce additional challenges. LTO-4 drives require the use of LTO-4 media to support encryption, preventing the use of existing tape inventories and requiring the creation of separately managed LTO-4 tape media pools. Replacing an entire inventory of existing tape media is usually not a viable option, and maintaining separate tape pools creates unwanted complexity.

Unlike tape drive-based encryption, however, CipherMax is compatible with any generation tape cartridge. Automated tape handling features can be set to turn off LTO-4 encryption when an LTO-3 tape is inserted, applying encryption using the CM device. An existing LTO-3 tape inventory can continue

to be rotated within the tape scratch pool, extending their life and allowing data to be migrated to secure, encrypted form over time. *KeyCruiser* provides a common key repository for all encryption keys, regardless of the tape media used.

M of N System Recovery

In the event of a system failure requiring a replacement unit, *KeyCruiser* works in conjunction with the *SANcruiser* management system to enable fast recovery of CM systems. CM systems can be recreated based on system configuration, security policy and encryption key data backed up in *KeyCruiser*, enabling the easy duplication of both system configurations and security parameters. A complete restoration of system data requires authorization from an 'M of N' quorum of recovery officers associated with that group of CM systems. This approach can be used to merge security domains, in the event of a broader system consolidation, or to regenerate new recovery keys due to organizational turnover or a periodic key rotation strategy.

Audit Logs

Increasingly, regulatory requirements and security standards require that audit logs be kept to provide irrefutable proof of administrative actions. *KeyCruiser* generates an audit log of all storage and security configuration changes and events, accessible for viewing only by authenticated security administrators. Audit log entries are held in secure, encrypted format that provides an integrity check, and can be securely exported to an external storage facility.

KeyCruiser Specifications

Management: Java-based GUI interface

Minimum System Specification: 1GB RAM, 40GB hard drive, 1 Ethernet connection

Architecture: Client-server application, supporting up to 16-way clustering

O/S Platform: RedHat Enterprise Linux 5 or SuSE Linux 10.2, Windows XP™ Professional, Windows 2003™ Server, Microsoft® Windows® 2000™ Professional and Windows 2000 Server.

Connectivity: TLS v1.0, SFTP

Role-based users: Security administrator, Recovery officers

Key Recovery: N of M quorum

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

