

## Solution Overview: SecureDR™

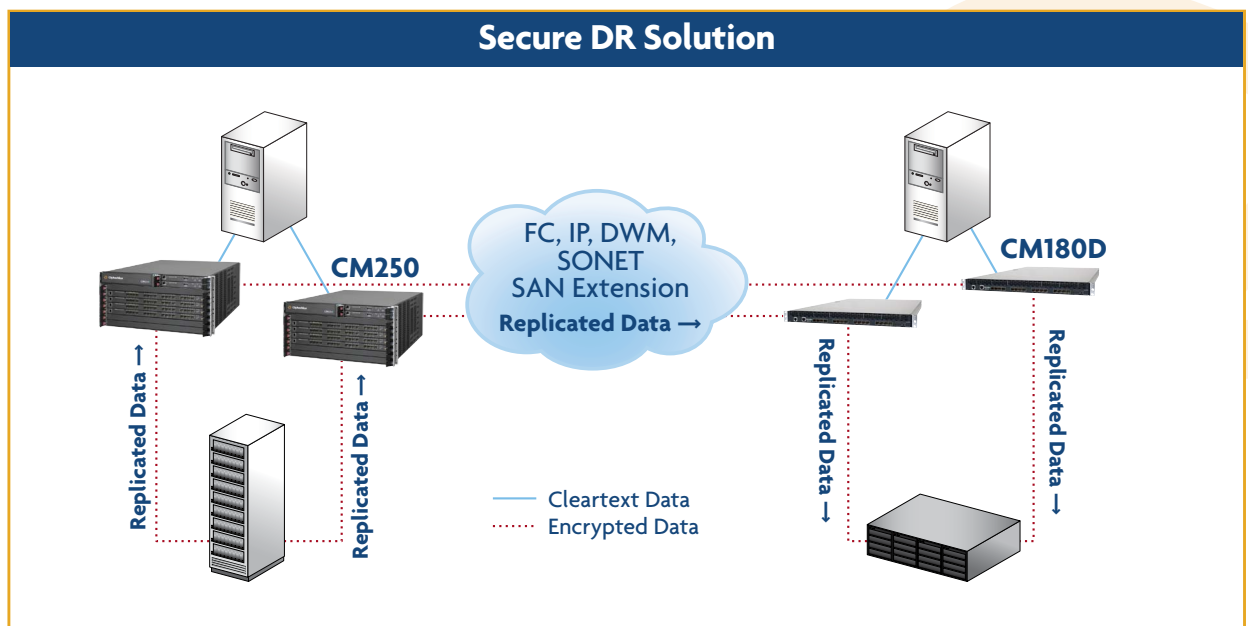
A Secure DR solution can be easily created by combining the Ciphermax cost effective storage security on disk solution with industry standard disk arrays. This combined solution ensures the secure replication, transmission and storage of sensitive data at remote sites for disaster recovery. SecureDR enables a quick time to recovery for primary data access to minimize downtime in the case of a catastrophic event, while greatly mitigating the vulnerability to data exposure at offsite or third party collocation facilities. The SecureDR solution provides:

- Transparent security with strong encryption of data at rest at local and remote locations
- Encrypted transmission of data across MAN or WAN links
- Convenient, single pane of glass management to minimize administrative overhead for distributed enterprise environments

### Why SecureDR?

Escalating requirements to protect the growing volumes of critical information from loss and corruption have accelerated the trend toward establishing offsite data replication (DR) sites, data repositories, and backup facilities. While these DR sites greatly enhance the ability to recover from a potentially disastrous loss of mission critical data, they also increase the number of points where an organization's information may be compromised. This expansion of data across multiple locations exposes several weaknesses in security strategies for distributed storage networks:

- The distribution of corporate information makes it difficult to apply selective encryption of data types like database columns, files, and email while ensuring the ability to later identify an associated key for data recovery.
- Traditional disk array or appliance-based data replication mechanisms do not provide an efficient method of encrypting data in transit over high bandwidth metro- or wide-area networks.



- Security at remote sites may not be equivalent to that of primary data centers. The use of third-party service providers to host or manage a replicate site exposes data to their personnel outside the control of the enterprise IT organization.

### What does the SecureDR solution include?

SecureDR adds a CipherMax CM180D for Disk system to an industry-standard disk array solution. In addition to the fabric-attached CM180D device, the CipherMax system includes the SAN*Cruiser* Network Security Management and the Key*Cruiser* Key Lifecycle Management systems.

### How does the CM180D install?

The CM180D installs between the backup server and the disk array as usual. The CM180D can be configured to be 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 CM180D's flexible installation options ensure SAN compatibility and easy installation and configuration.

### How does the SecureDR solution secure my replicate data?

As data is accessed from the primary storage for replication at the remote site, it passes through the CM180D device to be encrypted. The data is transmitted from the CM180D across the link to another CM180D and stored at the remote site while still in secure ciphertext form. This ensures the security of data both while 'in flight' between sites and 'at rest' at the remote location. The CM180D at the remote site provides decryption for

stored data in the event that it should be put into service as the primary site.

Encryption keys used to encrypt the data are shared between clustered Key*Cruiser* systems that maintain synchronized databases to ensure data recovery in the event of a local failure. The encryption keys can be also accessed by the remote CM systems once they are set up as trusted members of a shared security domain, enabling immediate recovery of cleartext data for failover operations.

### What is the impact on data replication operations?

The CM180D's line-speed throughput and optional deployment configurations ensure completely transparency to network operations with respect to performance, interoperability and replication processes. Hardware acceleration of data encryption processing and 16-ports of connectivity enable aggregate data transfer rates of 800MBps, vastly exceeding the throughput capabilities of most data replication servers.

### Do data replication sites have to be managed locally?

All security policy definition and key management can be done through a single management interface, saving time and eliminating potential confusion resulting from the manual transfer of encryption keys between key management systems.

### Where can I get more information on the SecureDR solution?

For more information, please contact CipherMax at [sales@ciphermaxinc.com](mailto: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](mailto:info@ciphermaxinc.com)  
**Partners:** [partners@ciphermaxinc.com](mailto:partners@ciphermaxinc.com)  
**Sales:** [sales@ciphermaxinc.com](mailto:sales@ciphermaxinc.com)  
**Technical Support:** 1-800-670-4423

#### WEBSITE

[www.ciphermaxinc.com](http://www.ciphermaxinc.com)

