ZECURION
Protection as a Priority™

Zecurion DLP Cloud

Zecurion Enhances the Capabilities for Protecting Data in the Cloud

Zecurion offers capabilities for the seamless and transparent encryption and protection of data stored in the cloud through its Zecurion Zserver. This product transparently encrypts real-time data as it is written to storage media, even in the cloud, and decrypts it when the data is read back. This allows the data to always be stored in an encrypted format, thus ensuring that it is not accessible by unauthorized personnel and/or a system that does not have the correct encryption key.

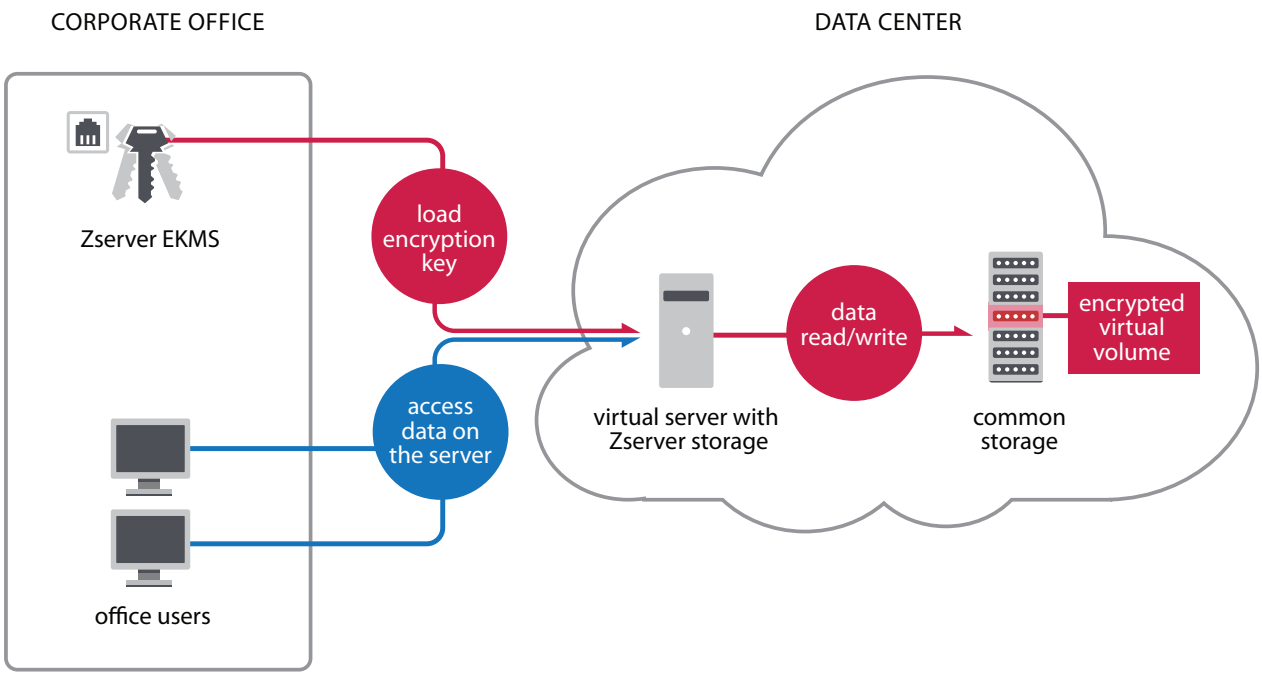
Using Zserver Storage in the Cloud

Each of the cloud-based servers used for processing sensitive data as a part of the standard environment and normal daily operations must installed Zserver. A separate, dedicated server (ideally a local server not in the cloud data center) must be allocated to function as the Zserver Enterprise Key Management Server (EKMS).

The Zserver EKMS stores all encryption keys used to encrypt and decrypt the data by the Zserver software on the cloud-based servers. Each of these cloud-based servers with Zserver installed must be registered within the Zserver EKMS in order to connect to the EKMS and load the encryption keys from it.

After this registration, all of the cloud-based servers running Zserver can automatically load the necessary encryption keys from EKMS and open encrypted disks. Only servers that are registered in EKMS by the system administrator can load the encryption keys. In addition, all traffic to and from the EKMS is encrypted so the keys are securely transported to or from the EKMS.

Servers running Zserver and registered in the EKMS automatically perform the encryption of the data on specified partitions. In case the server with access to sensitive data needs to be restarted, it will automatically reconnect to the Zserver EKMS, load the necessary encryption keys, and open the encrypted partitions to people with authorized access to those servers.



Access to encrypted data will not be possible by unauthorized users or applications. Even if the physical hard drive or storage media is lost or stolen, the Zecurion encryption will prevent unauthorized access to all encrypted data. In the event of a server restart, whether intentional or unexpected, the Zecurion encrypted virtual server will reconnect to the Zserver EKMS to authenticate the encryption keys and resume access to protected data.

Zecurion Zserver server encryption is only available for Windows 2000 SP4, Windows Server 2003 SP1, and Windows Server 2008 platforms. The Zecurion encrypted servers and the Zserver EKMS must be part of the same Windows domain or at least within the domains with an established trust relationship.

Manage Encryption Keys with EKMS

Encryption of data is by far the most secure way of protecting information by offering unparalleled security when implemented correctly. Until recently, this protection came with significant overhead for the encryption keys' administration and management. This is because encryption keys are not easily replaced or recovered. In fact, data encrypted with a strong algorithm and a long enough key are virtually unbreakable and irrecoverable if the key is lost. On the other hand, any disclosure of the key to an unauthorized party or a system can easily result in costly data breaches. Therefore, it is imperative for an enterprise to fully understand the encryption key management lifecycle before committing to a solution.

Centralized Secure Encryption Key Repository

The safekeeping of encryption keys is facilitated by a centralized repository encrypted by a master key. A master key can be generated using encryption key quorum (recommended). This provides enhanced security of keys used to encrypt a company's data. EKMS extends roll-based granular access management to both the repository and the keys, thereby allowing the segregation of duties, such as generating keys, accessing key properties, loading keys from EKMS, and performing other administrative tasks.

ZECURION

Protection as a Priority™

Encryption Key Quorum

The Zserver Enterprise Key Management Server (EKMS) is built by data encryption experts with deep knowledge and an understanding of the data encryption complexity and the key management challenges that organizations are facing today. EKMS was designed on the premise that no single entity should be granted sole possession of an encryption key. This is implemented by means of encryption key quorums. An encryption key quorum is a minimum required number of two or more key fragments to assemble the encryption key. For example, an organization can safely generate any number of key fragments (e.g., five) that are given to different employees and then set the quorum to two fragments. This will enable the organization to provide each system administrator with a single key fragment that requires at least two administrators to load the encryption key. This process effectively eliminates the dependence on any single staff member and abolishes the need to re-encrypt data when a key fragment is lost or an employee leaves the organization. Key fragments are stored on smart cards or other secure storage media.

Auto-Loading Encryption Keys

Server maintenance often requires servers to be taken offline and restarted, which causes encryption keys to offload from memory. While working with several servers may not impose significant administrative overhead, when operating hundreds or more, manually loading the keys is much more challenging. EKMS streamlines these tasks by automatically loading corresponding encryption keys when the servers are brought back online. EKMS ensures server authenticity by validating each server's certificate prior to loading the key and this avoids any network conflicts or changes in hardware.

Managing Cloud Security

Security in "the cloud" is a major obstacle that prevents many organizations from employing this computing service delivery model and taking advantage of operational and financial savings. By outsourcing all or some parts of its IT functions (or infrastructure), an organization often relinquishes the ownership and/or control over its informational assets to a third-party provider. This is a tremendous risk for many businesses, as they struggle to assess their cost savings against potential damages from data breaches or losses.

Using locally hosted EKMS, or smartcards to store encryption keys, organizations can safely encrypt data stored in the cloud while maintaining control over the keys needed to decrypt it.

For More Information

www.zecurion.com

304 Park Ave South, 11th Floor
New York, NY 10010

(866) 581-0999

For consultation or business enquiries:
info@zecurion.com