

# Veritas NetBackup™—Encryption Options

## Encryption options for offsite backup tape protection

---

### Overview

Companies lock buildings to protect their investments and secure networks to protect their data, but they often overlook the security of their backup and disaster recovery data. Backup and recovery information frequently mirrors existing corporate and customer data, making its security as important as primary sources of storage. When companies move unencrypted backup information by tape or disk to an offsite location, they expose private customer data, corporate financial data, and intellectual property to significant risk.

Headlines have highlighted one story after another of high-profile data security breaches. The challenge is clear: Data is mobile and therefore vulnerable. One backup tape can contain hundreds of thousands of confidential customer records. Data is shared with business partners, replicated to multiple data centers, and copied onto different media types that may ultimately be transferred to a third party.

A security breach in a company's data storage can result in not only public humiliation, but also business interruption, lost valuable assets, and reduced consumer confidence. The costs of losing customer information are becoming too high for companies to ignore, far exceeding the costs to protect it. In fact, a leading analyst says that protecting customer records can be as much as 15 times less expensive than paying for cleanup after a data breach or massive record loss.\*

A first step towards protecting company-sensitive data is to ensure that any backup tapes sent offsite for archival or disaster recovery purposes are encrypted. Veritas NetBackup allows administrators to centrally manage and track the encryption of backup data from within the NetBackup policy. By using software rather than hardware to control encryption, administrators gain a heterogeneous security option that allows them to encrypt and decrypt data regardless of the hardware platform used for backup or recovery. This also helps to lower capital and operational costs because no separate hardware encryption devices, dedicated staff, or changes to backup procedures are required.

Veritas NetBackup offers two options for encrypting backup tapes: the Client Encryption Option, which encrypts at the client/source for highest security, and the Media Server Encryption Option, which encrypts at the media server, providing easier management and a negligible impact on client performance.

---

### Features and benefits

- **Simplified management**—Administer the encryption process within the NetBackup policy with no change to backup processes.
- **Scalable**—Unlike hardware-based encryption solutions, software is scalable, so when environments scale, the encryption solution does too.
- **Flexible deployment**—Choose encryption point (client and/or media server) and type of encryption strength based on requirements and environment.

\* ITnews, "Cleaning up data breach costs 15x more than encryption," June 7, 2006.

- **Cost-effective**—No dedicated encryption hardware devices and no special training or changes to the backup process are required.
- **Asset protection**—Ensure company-sensitive material stored on backup tapes is encrypted before tapes are moved offsite.
- **Highly secure**—Maximum standards-based encryption strengths and centralized key management.

---

### Encryption made easy

NetBackup allows administrators to centrally manage and track the encryption of backup data from within NetBackup. No changes to backup processes are required, and there is no need to procure or manage dedicated hardware. By using software rather than hardware to control encryption, administrators gain a heterogeneous security option that allows them to encrypt and decrypt data regardless of the hardware platform used for backup or recovery.

---

### Client Encryption Option

For the highest security, the Client Encryption Option (CEO) encrypts data at the source/client so data is protected while in transit and in media. Ideal for protecting smaller, yet dedicated clients/databases, CEO can support disk or tape as a target. On restores, the encrypted data is read from media and transferred across the network to the client before decryption. A key file created using a pass phrase resides on the client and is required to decrypt encrypted data.

CEO provides data encryption using either 128-bit or 256-bit OpenSSL ciphers. This level of encryption meets both

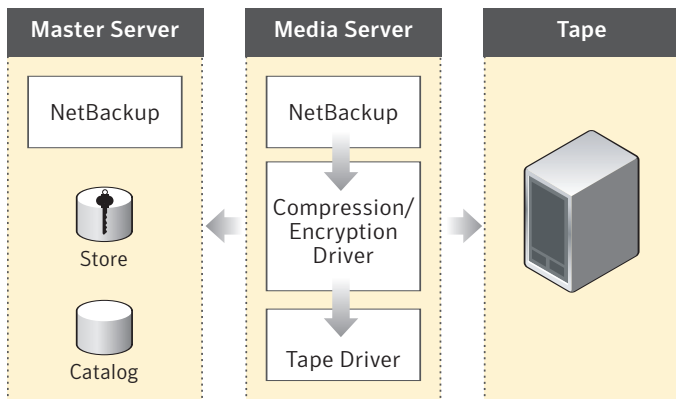
U.S. government and corporate standards of encryption quality. For organizations with legacy encryption options, CEO also supports 40-bit and 56-bit encryption methods.

### Media Server Encryption Option

For maximum flexibility and performance, the Media Server Encryption Option (MSEO) encrypts at the media server, avoiding impact to client operations. By providing parallelized and selectable encryption and compression, MSEO allows IT managers to choose the data to encrypt, the level of compression that is most appropriate, and the level of encryption key strength. In this way, encryption requirements can be customized so that they are aligned with overall business and service level agreement requirements. And because MSEO encrypts at the media server, it frees up critical client operations from CPU overhead and supports the most common backup configurations, such as disk staging to tape, the creation of tape copies for offsite purposes, and the backup of NAS devices (via NDMP).

For “set it and forget it” key management, MSEO offers automated key management that can be centrally located on the NetBackup master server. There is no need to manually track which key was used for which tape because it is automatically tracked. MSEO removes the burden of manual key/pass phrase management from the equation. This reduces complexity and saves administrative bandwidth as well as sets the stage for protection of the key store. Administrators can easily protect key stores by performing nonencrypted backups of this central location coincident with NetBackup catalog backups. And for the largest of environments, MSEO scales to accommodate multiple media servers in an environment.

MSEO offers a choice of encryption strengths for maximum security (AES 128-bit and AES 256-bit). For keys, MSEO provides centralized key management and hierarchical key security.



**Figure 1. The MSEO encryption driver resides between the NetBackup and tape driver layers of the backup architecture.**

As shown in Figure 1, the MSEO encryption driver resides between the NetBackup and tape driver layers of the backup architecture. In this instance, the NetBackup master server is the host on which the security server key management resides.

#### Additional MSEO Product Highlights

- Centralized management of the encryption process across multiple NetBackup media servers
- Encryption at the media server
- Integrated within the NetBackup policy for easier management and control
- High-performance parallelized encryption with minimal client impact
- Centrally managed key store for “set it and forget it” key management
- Choice of compression algorithms and standards-based encryption strengths
- Support for most common backup configurations, including disk staging to tape, the creation of tape copies for offsite purposes, and the backup of NAS devices (via NDMP)
- Scalability to accommodate multiple media servers in an environment
- PCI compliance

### NetBackup Client Encryption Option and Media Server Encryption Option feature comparison

Feature	Client Encryption Option (CEO)	Media Server Encryption Option (MSEO)
Encryption strength	DES: 40, 56, and 112 (2 triple key DES); AES: 128 and 256; Blowfish 128	AES: 128 and 256
Compression option	Uses NetBackup client compression feature	Selectable options: LZRW3, LZ01X, and TXT85.ENG
Encryption source	Client	Media server
Encryption target	Disk or tape	Tape
Management	Administer within NetBackup	Administer within NetBackup
Key management	Manual	Automated and centralized
Scalability	No logical limit; simply add client licenses	Centralized across multiple NetBackup media servers; no logical limit
NetBackup support	v. 5.1 and 6.0	v. 5.1 and 6.0

### Operating systems supported

For complete NetBackup software and hardware compatibility information, please see the Compatibility List at [www.support.veritas.com](http://www.support.veritas.com) or contact your Symantec sales representative or authorized Symantec reseller.

- IBM® AIX®
- HP-UX®
- Sun™ Solaris™
- Linux®
- Microsoft® Windows®

### More information

*Visit our Web site*

<http://enterprise.symantec.com>

*To speak with a Product Specialist in the U.S.*

Call toll-free 1 (800) 745 6054

*To speak with a Product Specialist outside the U.S.*

For specific country offices and contact numbers, please visit our Web site.

### About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

### Symantec World Headquarters

20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

