An Oracle White Paper
March 2011

# Encrypt, Protect and Secure Your Backup Data with Oracle Secure Backup

# Table of Contents

# Tape Backup Management

Reliable data protection in the enterprise extends beyond simple tape backup to multi-tiered data protection strategies meeting stringent business and regulatory requirements. For over 20 years, tape has been the cornerstone of data protection providing the most affordable, reliable media for long-term backup storage.

Enterprise environments manage 1000s of backup tapes with differing retention periods, storage locations and security requirements. Portability is a key advantage of tape over other types of backup media. For disaster recovery purposes, tapes are often shipped to an offsite storage location. Whatever the shipping method, boxes can be lost in transport. Lost backup tapes represent a real disaster for your company especially if those tapes contained sensitive user or business data – unless the backups on tape were encrypted!

This paper discusses how to leverage Oracle Secure Backup's encryption capabilities for protecting backup data on tape while in the data center, intransit, offsite or lost.

## Oracle Secure Backup – Introduction

Oracle Secure Backup (OSB) delivers unified data protection for heterogeneous environments. Protecting both Oracle databases and unstructured data, Oracle Secure Backup[1] provides centralized tape backup management for your entire IT environment:

- Oracle database via built-in integration with Recovery Manager (RMAN) supporting Oracle Database 11g, Oracle Database 10*g* and Oracle9*i*
- File system data protection: UNIX / Windows / Linux hosts
- Network Attached Storage (NAS) data protection leveraging the Network Data Management Protocol (NDMP)

The OSB Administrative Server centralizes backup management operations across distributed servers, NAS devices and tape devices. The configured hosts and tape devices managed through an Administrative Server comprise an OSB domain. With a highly scalable client/server architecture, Oracle Secure Backup domains may consist of one to hundreds of hosts (servers and/or NAS devices). As shown below, hosts within the domain may be direct or SAN attached to tape devices or backed up over the network.

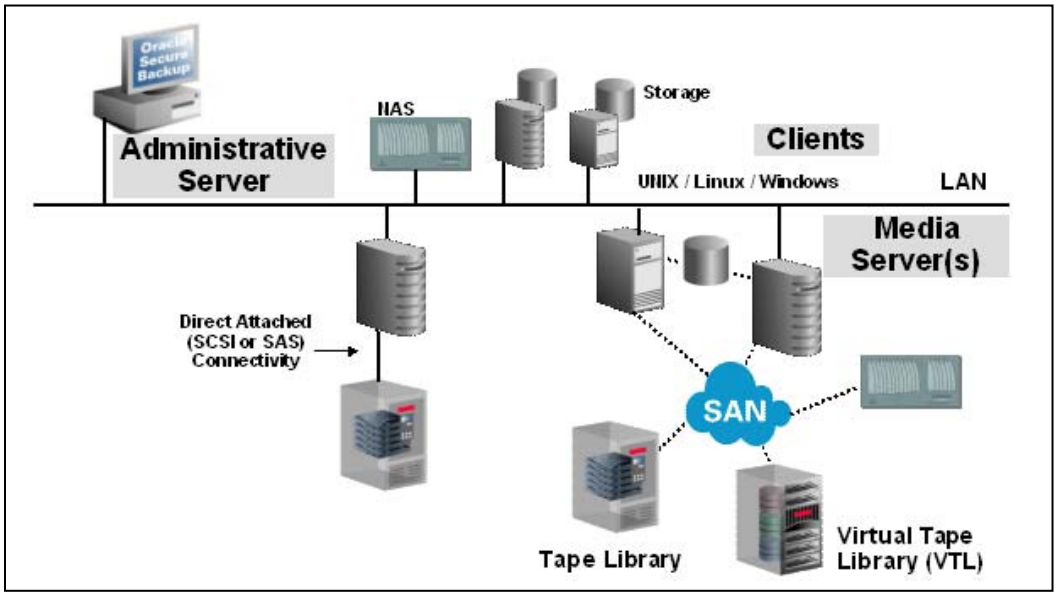


**Figure 1: An example of an Oracle Secure Backup domain configuration.**

[1] For more information on Oracle Secure Backup, please refer to www.oracle.com/goto/osb

The Oracle Secure Backup environment may be managed using command line, OSB web tool and/or Oracle Enterprise Manager (EM).

## Strict Security Controls for Backup Data and Domain

Data is the life-blood of business and must be guarded against malicious intent while in active state on production servers or preserved state on tape. Data center security procedures are critical in restricting physical access to servers, data, and company networks. As data is preserved onto tape, Oracle Secure Backup works in parallel providing strict security controls for protecting backup data and guarding access to the backup domain.

Unfortunately in today's world, no software can claim complete protection against malicious intent. Oracle Secure Backup's multi-faceted security offering combined with data center operational processes provide an interwoven security model for the backup infrastructure. Oracle Secure Backup security controls can be categorized into three areas:

- User-Level Access Control
- Host Authentication and Secure Network Communications
- Backup Encryption and Key Management

Securing backup data is of critical importance. Oracle's commitment to delivering reliable, secure software is evident in the rich set of security capabilities provided by Oracle Secure Backup.

### User-level Access Control

Oracle Secure Backup offers user-level access control based on configured OSB users, associated backup privileges (OSB classes) and operating system user privileges. During installation, the OSB admin user is automatically created with user-defined password and is assigned to the pre-defined OSB "admin" class which is analogous to a super user.

Additional OSB users may be configured by the admin user and assigned to one of six pre-defined classes or a new class may be created. While a user may be associated with only one OSB class, a class may be associated with multiple users.

The identifying user data and associated rights are cataloged and managed by Oracle Secure Backup providing a consistent user identity throughout the backup domain.

### Host Authentication and Secure Network Communications

Secure communication between distributed hosts within the backup infrastructure is essential. Oracle Secure Backup has embedded Secure Socket Layer (SSL) technology to guard against unauthorized access to the backup domain as follows:

- Two-way server authentication between UNIX / Linux / Windows hosts
- Encryption as part of SSL transport for secure transmission of OSB control messages and/or backup and restore data

During installation, an X.509 host identity certificate is automatically created and stored in an embedded Oracle wallet, which is exclusively used by OSB for storing host identity certificates. As certificate authority, the OSB Administrative Server digitally signs all host certificates automatically during installation.

Before performing any backup and restore operations, server identity is two-way authenticated using the X.509 host certificates; commonly referred to as an SSL handshake. A host identity certificate is used for securing communication between hosts within the backup domain and is not associated with the backup itself. If a host ID certificate were updated or eliminated, it would have NO effect on the ability to restore backup data originating from the host.

OSB control messages and/or backup data may be encrypted while in transit over the network utilizing SSL encryption. Upon reaching its destination, these SSL-encrypted messages and backup data are automatically decrypted by SSL. Security controls such as use of SSL is user-configurable in the security policies section of Global defaults and policies.

Note: Backups which were already encrypted by OSB or RMAN on the host will not be re-encrypted via SSL for transport over the network.

## Backup Encryption and Key Management

The recent rash of lost backup tapes has catapulted the need for backup encryption to the forefront. Addressing these security requirements, Oracle Secure Backup 10.3 provides policy-based backup encryption and key management. Backup encryption requirements may vary by host, backup or type of backup. Oracle Secure Backup offers three distinct backup encryption options:

- OSB host-based encryption:
  - Any backups from UNIX / Linux / Windows hosts
  - Encryption occurs on the host prior to transport (if any) over the network
- Tape drive[2] encryption:
  - Any backups from UNIX / Linux / Windows hosts and NAS devices
  - Encryption occurs on the tape drive itself
- RMAN backup encryption:

[2] Oracle Secure Backup supports backup encryption capabilities of LTO-4, LTO-5, T10000B and T10000C tape drives as listed on the tape device support matrix: http://www.oracle.com/technetwork/database/secure-backup/learnmore/tape-devices-10-3-161824.pdf

- Oracle database backups (available with Oracle Database 10g Release 2 forward, Enterprise Edition only)
- Encryption occurs within the database during the backup operation
- Oracle database (and not OSB) manages the encryption keys
- RMAN backup encryption directly to tape is available only with Oracle Secure Backup

Oracle Secure Backup manages the encryption keys for OSB host-based and tape drive encryption. Key management is identical for both methodologies as one environment may choose to utilize tape drive encryption for some backups and host-based, software encryption, for others. Oracle Secure Backup encryption and key management are applicable for file system and/or Oracle database (all supported versions and editions) backups.

## Policy-Based Management Infrastructure

Oracle Secure Backup includes a set of pre-configured global defaults and policies defining operational behavior within the OSB backup domain. These policies range from amount of time OSB logs are maintained to minimum password length required for OSB users. You may leave the existing default settings or modify as appropriate for your specific requirements.

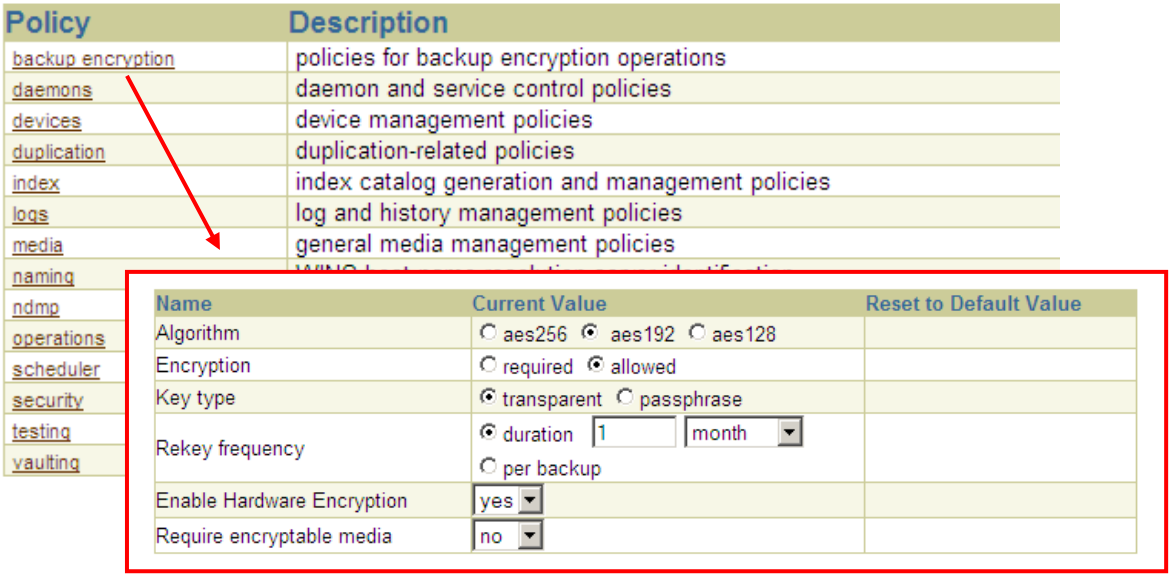


**Figure 2: OSB web tool screenshot of the global "Defaults and Policies" page with backup encryption options highlighted.**

Domain-wide (global) policies and defaults streamline operational consistency and minimize user-configuration efforts. Understanding the difference between global policies and defaults allows you to take full advantage of OSB's management infrastructure.

Global policies mandate specific behavior throughout the domain while defaults seed lower-level (ie host) policy default values from that point forward. For example, changing a global default value for a host related policy would affect new host configuration settings, but not the existing ones. Conversely, changing a global policy would be applicable across the board as it's a policy, and not a default setting. If a global configuration option may be defined at a more granular-level, then it is a default value for the lower-level and not domain-wide policy.

Oracle Secure Backup's policy-based management infrastructure begins with global defaults and policies providing the backup administrator fine-grained control over operational behavior across the domain. Theses operational defaults and policies can be equated to the backup management foundation. Beyond domain infrastructure, Oracle Secure Backup delivers a comprehensive set of user-definable policies for effectively managing media, backup encryption, hosts, tape devices and more.

## Host-based versus Tape Drive Encryption

With multiple encryption options available, which one or combination of strategies would best meet your data center security requirements? The answer is dependent upon your requirements. Host-based (software) and tape drive encryption each come with advantages and disadvantages.

The most commonly believed benefit of host-based encryption is that the backup is encrypted on the server prior to transport over the network. Depending on your requirements and environment, this capability of never exposing unsecured data on the network may be of utmost importance. Oracle Secure Backup can meet the requirement of securing backups prior to transport over the network in several ways:

- OSB native, host-based encryption
- RMAN backup encryption (Oracle database backups only)
- Encryption as part of SSL transport

Backup data encrypted as part of SSL transport is decrypted upon reaching the media server. The backups could then be encrypted by the tape drive or written to tape in clear text.

Probably the biggest drawback of host-based encryption is overhead on the server. Backup encryption and compression (if needed) are both CPU intensive operations. Why would compression come into play? Most tape backup environments leverage tape drive compression which is roughly 2:1 depending on data. Encrypted backups can't be effectively compressed by a server or tape drive. If compression is required, the host or tape drive must first compress then encrypt the backup.

The biggest advantage of tape drive encryption is reduced overhead on the host as compression and encryption are offloaded from the server. As compression is performed first, the ratio would be the same whether the backup is then encrypted by the drive or not.

There are two global backup encryption policies, as shown in figure 2, associated with hardware encryption:

- Enable Hardware Encryption – By default, Oracle Secure Backup will automatically leverage tape drive encryption (when available) versus host-based. If this setting is changed to "no", OSB will use only host-based encryption even when encryption capable tape drives are available.
- Require Encryptable Media (tape) – This policy is no, by default. Therefore, if a tape capable of encryption is not available, OSB will automatically leverage software encryption for the operation instead of tape drive encryption. If this policy is changed to "yes", OSB would place the backup job into pending status awaiting the user to input an appropriate tape. (Note: this policy is ignored if an encryption capable tape drive is not available)

## Encryption Key Management

It has long been said, "Encryption is easy; it's the key management that's hard". Oracle Secure Backup streamlines key management challenges via user-defined host policies applicable to both hardware and software encryption. All encryption keys are centrally stored on the Oracle Secure Backup administrative server in host specific key stores.

The host encryption key policies determine how OSB generates and manages the keys for encrypted backups performed on the host or via tape drive encryption. As discussed previously, global backup encryption defaults seed the host policies upon initial host configuration. The host encryption options are displayed below:

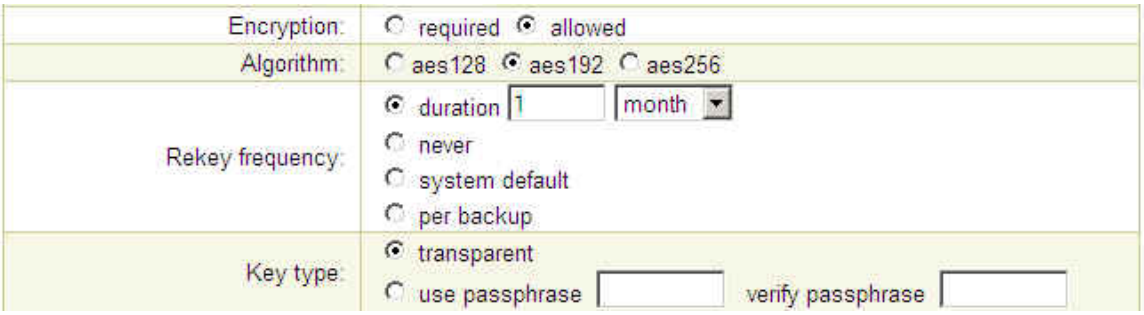


**Figure 3: OSB web tool screenshot showing host encryption policies.**

While similar to global options, the host encryption options are expanded for:

- "Rekey frequency" providing additional options to either "never" rekey or rekey per "system default" which then uses global rekey settings.
- "Key type" provides the ability to input a passphase which isn't available at the global level.

## Random or Passphrase Key Generation

Oracle Secure Backup generates encryption keys based on the defined encryption algorithm of AES128, AES192 (default) or AES256[3] and key type. Two key types are available:

- **Transparent** – Randomly generated encryption keys.
- **Passphrase** – User-defined passphrase is utilized to generate the encryption keys.

Randomly generated keys are generally considered to be more secure. After all, a passphrase can more easily be compromised as it could be communicated verbally or through written correspondence and inadvertently wind up in the wrong hands. Whichever key generation method is leveraged, it's important to protect and backup the encryption keys. This is particularly critical for randomly generated keys because if lost or destroyed the backup couldn't be decrypted. Conversely, if a passphrase generated key was no longer available the passphrase could be input to decrypt the backup during restore.

All backup encryption keys are centrally stored on the OSB Administrative Server in a directory comprised of host specific key stores. Upon OSB installation, users will define a password used to encrypt the keys store directory in the event the Administrative Server is compromised. Best practice is to backup the OSB Administrative Server on a regular basis.

During restoration of an encrypted backup, Oracle Secure Backup passes the appropriate encryption key from the Administrative Server via SSL to the client host for decryption. While decryption occurs on the host destination where restoration occurs, the encryption key is in temporary cache and never permanently stored on that host. Encrypted backups are automatically decrypted when restoration occurs within the same OSB domain for both transparent and passphrase encryption key types.

## Automated Encryption Key Regeneration per Policy

How often do you change passwords for logging into personal or company accounts? In fact, most corporations require employees to change their passwords on a regular basis. From a security perspective, older passwords have a higher risk of being compromised if for no other reason than the elapsed amount of time. Just as security best practice dictates user passwords be changed regularly, encryption keys should be as well. Oracle Secure Backup automates the process of updating encryption keys via the host's "Rekey frequency" policy, monthly by default.

Regenerating encryption keys on a regular basis limits exposure in the event that encryption key(s) were compromised. For example, if backup operations on host "a" were encrypted using one key for January, another key for February and so on, then a single "compromised" key could potentially expose up to one month of backups but not more. Conversely, if the same encryption key were used for years, that one key could decrypt years of backup data.

[3] Tape drive encryption leverages the AES256 encryption algorithm.

The rekey frequency policy is applied as follows based on the key type:

- Transparent – A new key will be generated automatically per rekey policy without user intervention.
- Passphrase – The user will be notified via email that a new passphrase should be defined to meet the rekey frequency policy.

Oracle Secure Backup maintains legacy and new encryption keys for seamless decryption of current or older backups in host specific key stores.

## Differences between RMAN and OSB Encryption

For Oracle database backup encryption, Oracle Secure Backup provides two-host based encryption options: RMAN (Oracle Database 10g Release 2 forward) or OSB software encryption. Both utilize the Oracle encryption library supporting algorithms AES128, AES192 or AES256.

There are some distinct management differences between the two which should be considered when determining which best suits your needs:

| **Oracle Database: Host-Based Backup Encryption Options** | | |
|---|---|---|
| **Description** | **RMAN** | **OSB** |
| Oracle database edition(s) / version | Enterprise / 10.2.0.1 forward | All / 9.2.0.1 forward |
| Encryption key generation | Oracle database:<br>• Transparent<br>• Password<br>• Dual | Oracle Secure Backup:<br>• Transparent<br>• Passphrase |
| Key storage | Oracle wallet for transparent and dual encryption key types | OSB Administrative Server in host specific key stores |
| Where encryption occurs | Within the database | On the database server |
| Configuration | EM backup schedule or RMAN | OSB database backup storage selector[4] or using the |

[4] Oracle Secure Backup database backup storage selector(s) establishes media policies for RMAN backups. For more information, refer to http://www.oracle.com/technetwork/database/secure-backup/learnmore/osb-103-twp-166804.pdf.

| | | |
|---|---|---|
| | parameters | OB_ENCRYPTION media management parameter in the RMAN backup script |
| Decryption during restoration | Varies based on key type:<br>• User inputs password for dual or password<br>• Automatically via accessible Oracle wallet for transparent or dual | Automatically, without user intervention, during restoration within the same OSB domain whether utilizing transparent or passphrase key types |
| Encryption Algorithms | AES128, AES192 or AES256 | AES128, AES192 or AES256 |

As discussed earlier, Oracle Secure Backup encryption policies may be defined at the host or global level with an encryption "required" directive. You, the user, determine which backup encryption method will be used to meet that requirement: OSB host-based, RMAN or tape drive backup encryption. If an Oracle database backup has been encrypted by RMAN, Oracle Secure Backup is aware of the encryption status and will not re-encrypt the backup to meet a "required" encryption policy.

## Configuring Backup Encryption

Encryption requirements for backup operations could be mandated across the domain, performed on an adhoc basis or somewhere in-between. Whether backup encryption is the exception or the rule, Oracle Secure Backup provides the configuration dexterity for it all.

Backup encryption may be configured via OSB global (domain-wide) or host policies, as part of backup scheduling or on a one-off, adhoc basis. Backup encryption is applicable to both Oracle database and file system backups although configuration settings vary between the two.

The following table provides an easy snapshot view of how to establish OSB backup encryption policies at various levels within the domain or to encrypt a one-time backup operation:

| **Requirement** | **OSB Configuration** |
|---|---|
| Encrypt every backup operation | Set the global encryption policy (as shown in figure 1) to "required" |
| Encrypt every backup operation from a specific host(s). | Set the host's encryption policy to "required" |
| Recurring file system backups | Encryption directive as part of the backup schedule |
| Recurring Oracle database(s) backups | Encryption directive as part of an OSB database backup storage selector |
| One-time file system backup | Encryption set as part of a "Backup Now" operation |

| | |
|---|---|
| One-time Oracle database backup | Use the RMAN media management OB_ENCRYPTION parameter in the RMAN backup script |

Whether encryption is configured per one-time backup, recurring schedule, encryption "required" setting at the host or global level, the encryption key policies established for the host will be utilized for its corresponding backups. The one exception to the rule is for file-system "transient" encrypted backups which leverage a user-defined passphrase supplied specifically for that backup operation.

Oracle Secure Backup provides the user-definable polices for consistent management and the flexibility to override said policies to accommodate those inevitable exceptions to the rule. Global and host encryption policies may be overridden at the backup level by using the "forced off" encryption directive as shown in figure 4.

## Transient Encrypted Backups

Periodically, a requirement may come about for backups to be performed at one location, followed by tapes shipped to an alternate location, and then restored. The backups need to be encrypted for security purposes along with an encryption key specific to those tapes. Transient encrypted backups address this requirement providing a one-off encrypted file system backup and designated encryption key.

Transient backup operations are evoked as part of a file system "Backup Now" operation:

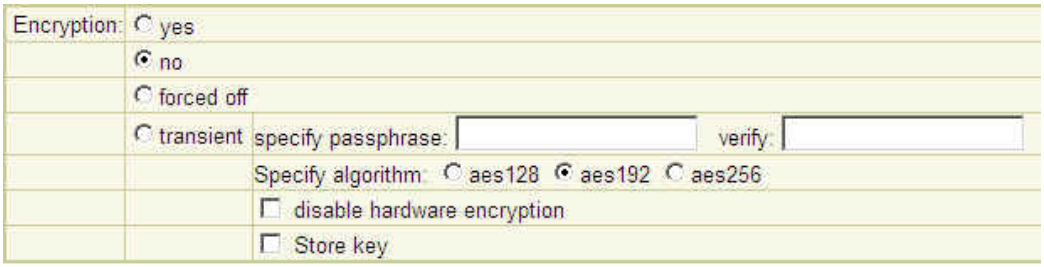


**Figure 4: Encryption options for a "Backup Now" operation shown via OSB web tool screenshot.**

A "Backup Now" operation configures a file system backup to occur immediately or at "x" time in the future but not on a recurring schedule. The encryption options associated with a "Backup Now" operation as shown in figure 4 are:

- "yes" – The backup will be encrypted using the OSB host(s) encryption key settings.
- "no" – The backup will not be encrypted (default).
- "forced off" – Turns encryption off for this backup operation by explicitly overriding any host or global encryption "required" setting.

- "transient" – The backup will be encrypted using the specified passphrase and encryption algorithm. In addition, you may select the following transient encryption options:
    - "disable hardware encryption" – By default, OSB will leverage tape drive encryption (if available). If these backups will be restored at a location that doesn't have the same type drives, you would want to leverage OSB host-based encryption therefore explicitly disabling hardware encryption for the backup.
    - "store key" – Encryption keys generated for transient backup operations are not automatically stored by default. If the "store key" option is designated, OSB will store the key in each of the host key stores which were part of the backup.

With transient encryption, one encryption key will be generated for the entire backup operation which may include data from multiple hosts. This differs from OSB standard encryption key management which uses a separate key per host that is included in the backup.

The primary use case for transient encrypted backups is when the backups will be restored at an alternate location and therefore different OSB domain. Since the alternate OSB domain catalog would be unaware of these volumes or backups, the first step in restoration would be to import the volume and associated backup metadata into the new OSB domain catalog. For restoration, you would input the passphrase along with encryption algorithm to decrypt the data.

## Summarizing – Why Secure Your Backup Data with Oracle Secure Backup?

It's often said that a backup protects your data while an encrypted backup secures and protects your data, your job and your company. All things being equal most would choose to protect and secure backup data. The question is how and the answer is Oracle Secure Backup.

Backup encryption can be accomplished in many ways. For example, you could purchase an inline backup appliance(s) which sits in the backup stream purportedly transparent to the backup software or perhaps encryption key software which is integrated with your tape drives. Both are viable encryption methods, no doubt. However, these offering often come with hefty price tags and add another moving part to your backup infrastructure. Who needs the added cost and complexity?

Backup encryption is one of the many OSB enterprise-class features. Oracle Secure Backup provides centralized tape backup management for your entire IT environment easily scaling from 10s to hundred of servers and 1000s of backup tapes. As with all of OSB's advanced functionality, backup encryption is included in the $3500 per tape drive licensing fee.

Backup encryption requirements vary by environment, host or backup. Oracle Secure Backup delivers the depth to meet your simplest to most complex backup encryption requirements:

- Two host-based backup encryption options:
    - OSB native backup encryption

  - RMAN backup encryption
- Tape drive encryption support for LTO-4, LTO-5, T10000B and T10000C drives
- Policy-based encryption key management
  - Transparently or passphrase generated encryption keys
  - Rekey frequency policies for automated key regeneration
- Multi-level backup encryption policies and configuration options:
  - Global and host encryption settings
  - Backup encryption defined as part of a recurring schedule
  - One-off, adhoc, backup encryption for those every once in awhile encryption needs

Oracle Secure Backup delivers data protection for the enterprise at over 75% less cost than comparable products. Unprecedented in the backup industry, OSB offers low-cost, single-component (per tape drive) licensing making affordable, secure data protection within reach of both small and large IT organizations. With Oracle Secure Backup, you can reduce IT costs without sacrificing functionality.

## Conclusion

Secure data protection from server to tape is crucial for local and offsite storage of mission-critical data. The portability and long-shelf life of tape is ideally suited for long-term, offsite backup storage. This advantage has a double-edge in that once backup tapes leave the safety of a secure data center; they are exposed to external variables and potentially 3rd party transportation or storage vendors. Oracle Secure Backup provides policy-based backup encryption securing the backup data on tape whether those tapes are onsite, offsite or lost.

What would it cost you and your business if mission-critical backup data fell into the wrong hands? When you consider the financial costs along with potential reputation damage, can you afford not to encrypt important backup data? Avoid unnecessary costs by encrypting, protecting and securing your backup data with Oracle Secure Backup.

White Paper Title: Encrypt, Protect and Secure your Backup Data with Oracle Secure Backup
March 2011
Author: Donna Cooksey
Contributing Authors: Ashish Ray

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment



0109