

Complete Online Microsoft Exchange Server Data Protection

**VERITAS NetBackup *for Microsoft Exchange* Best Practices Guide**

**July 2005**

**Table of Contents**

Executive Summary ..... 3  
     *Key Features: NetBackup for Microsoft Exchange:* ..... 4  
     *NetBackup for Microsoft Exchange Highlights*..... 4  
 Why protect Microsoft Exchange Server? ..... 5  
     *Why Do you Need VERITAS NetBackup for Microsoft Exchange Server?* ..... 5  
 Best Practices for Protecting Microsoft Exchange ..... 6  
     *Application Protection – protecting Exchange files and settings* ..... 7  
     Best Practices for Exchange Deployment ..... 7  
     *Database Protection for protecting Exchange databases and logs* ..... 8  
     What Exchange backup method should be used, and when? ..... 10  
     Best Practices for Exchange Database Recovery ..... 10  
     *Mailbox-Level Backups* ..... 11  
     Optimizing Mailbox-level Backups ..... 11  
     Mailbox-level Backups with VERITAS NetBackup for Microsoft Exchange Server..... 12  
 Other Exchange related Solutions from VERITAS ..... 13  
 Summary ..... 14

## EXECUTIVE SUMMARY

The steady march of new, innovative storage software capabilities continues to revolutionize information in many ways: from availability to recoverability to manageability. As storage capacities continue to explode, so do the demands for advanced, tightly integrated storage management solutions. Along with having a growing amount of data and information, customers are demanding total storage management solutions that have a high level of functionality and performance, ideally if these requirements can be achieved without impacting the availability or performance of production applications. Nowhere are these demanding requirements more visible than when supporting Microsoft Exchange environments that allow customer to fully exploit the full potential of Microsoft and VERITAS products for highly available and recoverable Exchange Server configurations.

Every new release of Microsoft Exchange Server offers new and innovative messaging options: from electronic mail, voice mail, video conferencing and instant messaging. However, as customers plan for new ways to exploit these new Exchange Server features, the need to examine their underlying technology infrastructure becomes even more challenging and complex.

The critical issues affecting Exchange Server deployments today are availability and recoverability. With ever-greater reliance on any form of electronic communications, anything that could cause an Exchange Server outage quickly becomes a potential business disaster. The harsh realities of today's global business require that Exchange Server environments be designed and implemented using the latest storage management features to ensure the highest levels of availability and recoverability.

The critical business information residing within production Exchange Server databases requires periodic backup to protect against data loss or corruption. More frequent backups permit faster recovery time. However, more frequent backups may impose a significant impact on the performance and availability of Exchange databases. Because of the tremendous availability and accessibility requirements imposed by today's electronic commerce, databases, such as Exchange Server, cannot tolerate any downtime caused by traditional backup methods.

Too few backups result in a too long and often cumbersome recovery process; too few backups may degrade overall system availability and performance. This raises a difficult question affecting many enterprises today:

*How can customers protect business critical Exchange Server databases without imposing any performance or availability limitations on their production computing systems?*

Fortunately, improvements in storage management software can allow customers to design, implement and manage even the most complex and data intensive environments, often without acquiring new storage hardware.

There are many compelling reasons why customers need to implement improved storage management solutions in support of Microsoft Exchange Server, with business continuity, or the ability to keep critical business computing assets available and recoverable, are the two most important.

This white paper will address several aspects of an Exchange Server data protection plan, focuses on how VERITAS NetBackup for Microsoft Exchange meets the needs of this plan, and introduce several critical best practices for comprehensive protection of Exchange databases and services.

VERITAS NetBackup for *Microsoft Exchange* is the highest performing and most flexible way available to protect Microsoft Exchange server data while keeping Exchange fully available. Providing full backup and restore of all Exchange Server components, including embedded objects, attributes, and all Outlook components, **NetBackup for Microsoft Exchange** also gives administrators the flexibility to perform individual mailbox backup with selective restore down to an individual message.

### Key Benefits

- Helps safeguard the integrity of critical corporate Microsoft Exchange Server data.
- Incorporates online nondisruptive Exchange Server database protection as part of everyday backup routines, which increases the chance of data recovery and minimizes data loss without inhibiting daily activity.
- Protection of individual mailboxes gives administrators the ability to perform granular restores down to a single message.

## KEY FEATURES: NETBACKUP FOR MICROSOFT EXCHANGE:

- **NEW! Off-Host Exchange Backup** – Exchange backups can be performed at any time – even at peak production times – without impacting e-mail performance or responsiveness.
- **Single Instance Storage of Message Attachments** – excludes duplicate attachments delivering faster backups of individual mailboxes by eliminating backup of duplicate information.
- **Greater Flexibility** – Exchange backup administrators can now perform incremental backups of individual mailboxes and public folders when performing mailbox-level backups.
- **Specific Folder Exclusion** – provides Exchange backup administrators the ability to globally include or exclude specific folders, select or deselect common folders as well as define include or excludes by typing the folder names during Exchange mailbox backups.
- **Individual Public Folder Restore** – provides Exchange backup administrators the ability to select individual messages and folders from public folders during a restore.

## NETBACKUP FOR MICROSOFT EXCHANGE HIGHLIGHTS

- **Complete non-disruptive protection of Exchange data:** transparently protects all Exchange Server Information Store and Directory data objects, including transaction log files, while keeping Exchange Server online and available.
- **Integration:** Uses the native Exchange Server Backup APIs and Messaging APIs for reliable Exchange protection
- **Completeness and coverage:** NetBackup can backup and restore at the storage group level, as well as backup and restore databases within a single storage group. The Microsoft Exchange Key Management Service and Exchange Site Replication Service databases are also protected.
- **Automatic transaction log maintenance:** Exchange records all transactions into one or more transaction logs to maintain a record of all Exchange database operations. **NetBackup for Microsoft Exchange** automatically truncates committed transactions upon successful backup, ensuring transaction logs do not run short of available log space.
- **Restore Individual Exchange Mailboxes, Folders, or Messages:** Through the use of mailbox-level backups, recovering individual messages no longer requires a separate Exchange Server. Simply use the graphical interface to browse and select the specific mailbox and execute the restore task.
- **Automated Backup:** Help to define frequency or calendar-based schedules for automatic and unattended backups.
- **LAN-Free Exchange Server Backup:** Supports storage area networks backups with the NetBackup Shared Storage option, increasing backup and recovery performance over a fibre channel network and allowing for greater usage of shared tape devices.
- **Supports all Exchange Server Backup and Recovery Methods:** VERITAS NetBackup for Exchange fully supports all Microsoft Exchange Server backup and recovery methods: full, cumulative incremental and differential incremental.

## **WHY PROTECT MICROSOFT EXCHANGE SERVER?**

In order to maintain Microsoft Exchange's availability and protect its data stores, a working and thoroughly tested data protection and recovery plan and reliable data protection software are essential. Together, they ensure the recovery of the Exchange Server system environment, user configuration data and/or message content in a timely fashion. The objective is to help minimize downtime for the enterprise messaging environment and to provide the quickest possible data recovery in the event of a system crash, database corruption, loss of a single mailbox, or other forms of data loss.

## **WHY DO YOU NEED VERITAS NETBACKUP FOR MICROSOFT EXCHANGE SERVER?**

Protecting a large application server like Microsoft Exchange requires careful thought and planning in order to meet the availability needs of your company and its budget. The most common method of formalizing these needs is the implementation of Service Level Agreements. These agreements are contracts between the users and providers (e.g., IT departments) that outline such factors as: expected services, acceptable downtime, and response time for problem resolution. It is critical that you understand these factors during the design phase of your Exchange deployment, as they can heavily influence the resources you'll need to support the plan.

## BEST PRACTICES FOR PROTECTING MICROSOFT EXCHANGE

### OVERVIEW

With most database applications like Exchange Server, data protection can be divided into two main objectives – preparing for a disaster recovery where all data (i.e. Windows operating system, Exchange Server application and its database) is destroyed, and preparing for the restoration of all or some of the application's database data.

Disaster recovery preparation includes protecting the Windows operating system and System State, the Exchange Server application directory, and database backups of Exchange, which is the focus of this white paper.

Since all user data is contained in Exchange Server's databases, protecting them is the main objective. Exchange Server provides several methods to backup and restore this data, but consider the pros and cons of each in order to achieve your data protection goals. There are two basic ways to protect Exchange Server data: (1) at the database-level and (2) at the mailbox-level. Database backup is mandatory, as restoring a database is the only way to retrieve all of the Exchange Server data back in times of disaster. Mailbox-level backup is optional, but it is highly advantageous when the data protection requirements demand fast recovery of specific messages or a user's mailbox.

In summary, data protection for Microsoft Exchange can be divided into three related categories:

- **Application Protection** – this includes backup and recovery of Exchange Server's application files, clustering support for Exchange, and Disaster Recovery procedures to recover the entire application as a necessary first step toward disaster recovery.
- **Database Protection** – this includes the protection of the Exchange Server data using methods such as backup and restore of database volumes within the Exchange Server storage groups/databases, also required for ensuring the ability to recovery from a disaster.
- **Mailbox-level Protection** – this includes techniques for the granular protection of Exchange data down to the individual mailbox (mail messages and attachments) for quick retrieval and minimal impact on systems or networks.

## APPLICATION PROTECTION – PROTECTING EXCHANGE FILES AND SETTINGS

At the application level, the focus is to protect the Exchange Server's application files and settings, along with presenting some options for protecting the entire application. Listed below are a few requirements, options and recommendation for protecting Exchange.

### Best Practices for Exchange Deployment

**Backup the Host Server for Exchange** – The single most important thing you can do to protect Exchange Server is to have regular, verified, online backups. This is critical as it forms the base for any reliable disaster recovery plan.

Since Exchange Server runs on Windows, protecting the underlying Windows operating system and Exchange Server's files and settings are very important for timely disaster recovery. This includes backing up all files on the volumes that Windows and Exchange are installed on, and backing up the Windows System State, which contains critical Exchange Server configuration information. The backup schedules of this data should coincide with the backups of Exchange Server databases creating a consistent set of data for an easier disaster recovery.

VERITAS NetBackup *for Microsoft Exchange* software communicates using Microsoft's Extensible Storage Engine (ESE) application programming interface, to perform standard Exchange database backup and restore. Mailbox-level backups and restores are accomplished through the use of Microsoft's Messaging application programming interface. Through these interfaces, NetBackup software coordinates all data movement and transaction log maintenance. During restore operations, NetBackup *for Microsoft Exchange* extracts the proper data objects off backup media and automatically replays the transaction logs to return Exchange Server to the desired recovery point.

**Backup the Active Directory** – Make sure that Active Directory, which contains most of the server configuration information, is backed up regularly. Additionally, you should deploy multiple domain controllers throughout each Active Directory domain to ensure full Active Directory replication so that if a domain controller fails, Active Directory services continue to be available. For Exchange Servers running Active Directory, the guidelines stated above to backup the Exchange host server would automatically backup the Active Directory database with the System State backup. If the Exchange Server is not running Active Directory, then select to backup the System State on a server running Active Directory. Attempt to schedule the Active Directory backups as close to the backups of Exchange Server data to create a consistent data set around the most recent server and operating system settings.

### Define your backup and restore requirements – create and review your recovery plans

- Your Exchange deployment plan is directly related to the disaster recovery strategy you plan to implement. Your deployment choices will affect your Exchange backup and restore options. Although the Exchange deployment strategy you implement affects the disaster recovery method you will use, the detailed discussion of disaster recovery strategies is outside the scope of this paper. For more information about Exchange deployment strategies and how they impact backup and restore planning, see the *Microsoft Exchange Server Resource Kit* or contact VERITAS Software.
- The Exchange deployment strategy you choose must coincide with the administrative skills within your company. Learning a little more than you think you often yield a high return if ever needed when facing a significant disaster recovery or crisis.
- Clearly define your backup and restore resource requirements, and periodically review and test your plan.
- In order to restore a consistent snapshot of backup data during disaster recovery, a good strategy is to coordinate the **full** backups of the Windows operating system files, Exchange Server application files, and the Windows System State with the full backups of Exchange Server's database. Follow this strategy for **differential or cumulative** backups of files and database backups too. If this cannot be accomplished, at

least backup the Windows System State with each Exchange Database backup – as it will not add much time to your backup and will provide a higher degree of protection for a disaster recovery later.

- Have a full, separate Exchange configuration that can be used for emergency recovery or configuration testing purposes.
- Do not use any open file agents when performing any Exchange database backups.
- To help minimize the amount of time it takes to backup and restore Exchange data, you should consider establishing size limits for mailboxes and public folders. You should also plan to store Exchange databases across multiple storage groups for optimal concurrent backup and restore performance.
- Test your Exchange data protection and disaster recovery plan often. Be certain to periodically check your backup media to ensure that you can read from it before an emergency restore is needed. Consider implementing VERITAS NetBackup Vault to proactively manage backup images stored in offsite locations.
- Avoid making the Exchange Server a Domain Controller. For disaster recovery purposes, it is much easier to restore Exchange if you don't have to first restore the Active Directory or Primary Domain Controller.
- Do not install Exchange into a domain that does not have at least two Domain Controllers. Database replication is not possible with only one Domain Controller in a domain. If the Domain Controller fails and corrupts the Active Directory, some transactions may not be recoverable if they were not included with the last backup. With at least two Domain Controllers in a domain, databases on the failed Domain Controller can be updated using replication to fill in missing transactions after the database backups have been restored.
- Make certain that your Internet Information Store (IIS) metabase is backed up. Should the entire Exchange server need to be restored, the IIS metabase must be restored to the Windows server before the Exchange server application data can be restored.

**Hot Backup of the Key Management Database and Site Replication Service Databases** – If these Services Databases have been deployed, then include them, each is normally very small, into the Exchange Server backups. Both will be protected using the same backup method that you selected for Exchange Database.

## DATABASE PROTECTION FOR PROTECTING EXCHANGE DATABASES AND LOGS

Exchange Server has two main databases for user information – the Directory and Message Store.

The Message Store is where user data is stored. This Store is actually two databases – Public (i.e. where Public Folder Data is stored) and Private (i.e. where user mailboxes are stored). To provide better support for scalability, clustering, and data protection, Exchange Server allows the Message Store to be split into several Storage Groups of databases serving specific users. Each Storage Group can be protected individually and shares transaction logs between databases within the Group, thus providing a more flexible data protection scheme.

The Directory Store is the database of users (recipients) within Exchange. In Exchange v5.5 and earlier, the Directory Store was part of Exchange. With Exchange 2000 and later, the application uses Active Directory for the user database. As a result, Exchange must run on Windows in an environment where Active Directory is used. Although data in the Directory Store doesn't change as much as the Information Store, it is critical that the Directory Store be protected in same backup schedule as the Information Store to maintain consistency between users and their data within the Exchange databases.

Exchange uses transaction logs for each database (i.e. or shared within a Storage Group) allowing the protection of Exchange in a highly granular manner via incremental or differential backups of the logs. Transaction logs are files containing a running log of changes to a database. To recover from error or corruption, Exchange can “replay” these logs back into the database up to the last successful transaction. As you can guess, Exchange Server can generate quite a few transaction logs very quickly if the Exchange server is busy. To control log

growth, frequent Incremental or Full backups are required since Exchange Server deletes the log files after these types of backups. Exchange Server offers a Circular Transaction Log mode that causes Exchange to use a small group of transaction logs that are overwritten in a circular pattern. While this has the benefit of requiring less log space since it overwrites the oldest log file in a circular manner, it also has the major disadvantage of **not** allowing incremental or differential backups of the Exchange Server.

**Online Backup of the Exchange Message Databases** – Since it has been established that messaging applications are considered very important and even mission critical to some businesses, it is critical that Exchange is always available. To meet this need, Exchange offers a method of performing an on-line or hot backup of Exchange databases which backup applications can interface with. This interface allows several backup methods such as:

- **Full Backup** – Full backups are the foundation backup type which complex and scaleable backup schemes can be based off of. If given a choice of only one method of backup choose a full. On-line backups have the added benefit of automatically deleting transaction log files upon successful completion of backup tasks. If possible, performing a daily full backup is Microsoft's preferred method for protecting Exchange environments.
- **Differential Incremental** – A differential backup will only capture changes since the last full or differential backup. This method can be used on Exchange databases, the KMS and SRS services, mailboxes and the Public store. Transaction logs are preserved and then deleted after backup. The advantages of this method is that it backs up the least amount of data and therefore has the smallest performance impact on the Exchange Server, while helping to conserve log file space. A disadvantage is that all incrementals must be restored consecutively after restoring a full backup. Circular logging, which shouldn't be used with Exchange 2000 and later, must be disabled in order to perform differential backups.
- **Cumulative Incremental** – Cumulative backups are similar to differential backups in that they back up only the transaction log files. The primary difference is that when using this method to back up Exchange databases, only transaction logs are backed up and they are not truncated upon completion of the backup. Transaction logs remain intact since the last full backup. Unlike differential backups, cumulative backup allows the log files to continue to grow larger, so you should expect daily differential backups to take progressively more time to complete. **The key advantage of a cumulative backup over a differential backup is found at restore time – restoring Exchange data will be faster and easier when restoring from a cumulative backup image.**

## What Exchange backup method should be used, and when?

<b>Full</b>	<b>Ideally performed daily, with larger sites performing a full backup 2-3 times per week along with some form of incremental backup.</b>	<b>Ideally per each Exchange storage group. Captures Exchange database and stream files and truncates transaction logs.</b>
<b>Differential</b>	<b>Ideally, differential backups should be performed at least once per day depending on service level agreements. Often performed several times per day to minimize backup impact.</b>	<b>Often workload dependent, this backup method captures Exchange databases and truncates transaction log files.  Should not be used with incremental backup methods configured for the same policy. Sites should use either differential or incremental only, not mix both.</b>
<b>Cumulative</b>	<b>Frequency based on service level agreement or restore requirements.</b>	<b>Fastest restore performance.</b>

## Best Practices for Exchange Database Recovery

- **In small office environments** with relatively small numbers of messages passing through the system, a daily full backup at night will provide sufficient data protection and the quickest recovery. If log file growth becomes an issue, consider using incremental backups each day to provide an added recovery point and manage the log file growth for you automatically.
- **In medium - large environments** many shops run full backups on the weekend and incremental backups during the week or intraday. If you have sufficient disk space for a week's worth of log files, then consider implementing differential backups during the week. While it's possible to schedule backup tasks to be executed several times per day or week, it's best to keep the scheme as simple as possible to make disaster recovery manageable.
- **In large environments** – Consider implementing multiple Storage Groups and backing each group up on a separate schedule or in parallel to separate tape devices for better performance if your server can handle heavier I/O workloads. Exchange 2000 and later supports up to 4 groups with 5 databases each. For example, separate mailbox users by department or last name into two Storage Groups which could be backed up by with two high performance tape drives to reduce your backup window. Implementing Storage Groups enables greater flexibility and performance while adding complexity to Exchange Server administration; see the Exchange Server documentation for guidelines for correctly implementing this feature.

## MAILBOX-LEVEL BACKUPS

Conventional Exchange database-level backups, while suitable for recovering an entire database or storage group, do not allow more granular restores down to an individual message or mailbox. Mailbox-level backups are backups that preserve each mailbox separately, allowing individual mailboxes or messages to be restored. With today's greater focus placed on historical email retention by regulatory agencies, businesses are faced with satisfying both disaster recovery needs and single message restore requirements. The only way to achieve both with Microsoft Exchange is to include both backup methods in the overall Exchange data protection strategy. There are two important factors to consider when incorporating mailbox-level backups into your overall data protection strategy:

- **Two separate backups must be performed on the same data.** Both database-level and mailbox-level backups must be performed in order to allow both database and message-level restores. Database backups do not allow granular restores of individual messages, while mailbox-level backups cannot be used for complete database restores or for disaster recovery, because certain meta-data in the database cannot be backed up through the MAPI interface.
- **Mailbox-level backup throughput is sub-optimal.** All mailbox-level backups must utilize the Exchange MAPI (Messaging API) interface. This is the only interface capable of mapping messages and attachments to users and mailboxes. Unfortunately MAPI was optimized to handle random email traffic, not the heavy loads generated by a backup operation. As a result, the raw backup throughput through MAPI is inferior to the backup throughput achievable through the ESE API, the Exchange interface optimized for database backups. The difference in transfer rates between mailbox-level and database backups can be significant. In one example, database backups would easily exceed 10 MB/second, while mailbox-level backups on the same database would barely reach 3 MB/sec.

Since these limitations are a result of the design and structure of Exchange, they exist regardless of the specific backup technologies used. There are ways to optimize mailbox-level backups to shorten the duration, but all mailbox-level backup technologies must work within these same two fundamental limitations.

### Optimizing Mailbox-Level Backups

Despite the increased burden mailbox-level backups can place on resources and time, there are some suggested best practices that will reduce this burden so that mailbox-level backups can be managed effectively along with database backups:

- **Backup a smaller selection of mailboxes.** The easiest way to limit the duration of mailbox-level backups is to limit the number of mailboxes being protected. Not all users need message-level restore capability, or IT may choose to limit message-level restore service to certain members of upper management, such as the CEO or the executive staff.
- **Exclude non-critical messages from backups.** A significant percentage of email may be part of the Deleted Items or Sent Items folders. Although this data is retained as a convenience for the user, it often makes no sense to backup this data, depending on the objectives of the business. Globally excluding these items can substantially reduce backup times.
- **Stagger backups of mailboxes.** Rather than backing up all mailboxes every day, break up users into smaller groups (e.g. one group for every day of the week) and backup only one group each day. The risk to this approach is that each user's mailbox is backed up less often, but this may be acceptable depending on the restore and data retention requirements. For example, if mailbox-level backups are to be used solely for long-term data retention to meet regulatory requirements, backing up every mailbox every day may be unnecessary and redundant.

- **Perform incremental backups of mailboxes.** This limits the scope of a typical mailbox-level backup to include only new email that has arrived in the last day or two, reducing the duration of a mailbox-level backup to perhaps 10-20% of a typical full mailbox-level backup.
- **Eliminate redundant data protection.** Without special technologies to identify identical objects within the Exchange database, a mailbox-level backup has the potential to become extremely redundant. For example, when a user emails a large distribution list, that same email may be protected multiple times, increasing backup times and backup storage (e.g. tape) utilization. As further detailed below, VERITAS NetBackup software can identify identical data within Exchange and protect that data once per database rather than once per user.
- **Perform multiple backups simultaneously.** Performance improvements can be achieved by backing up multiple mailboxes in parallel. Multistreaming and multiplexing technologies allow backups to be split into multiple data streams and targeted at one or more tape or disk storage devices. Database backups could also be executed at the same time as mailbox-level backups. Some tuning may be necessary to realize the optimal number of data streams depending on the specific details of the environment.
- **Implement mailbox size limits.** One more way to reduce mailbox backup time is to reduce the size of each mailbox by implementing mailbox size limits through Exchange. This forces the mailbox owner to delete email on a regular basis. Ironically, this approach could result in increased data loss and more frequent restore requests, as users will be forced to delete email that they may not realize they will need in the future.

### Mailbox-Level Backups with VERITAS NetBackup for Microsoft Exchange Server

VERITAS NetBackup for Microsoft Exchange software provides all the flexibility needed to optimize mailbox-level backups using the techniques discussed above. Some of the highlights of NetBackup for Microsoft Exchange software's capabilities include:

- **Single Instance Storage (SIS)** – It is estimated that between 70-90% of data within a typical Exchange database is attachment data. To conserve space, Exchange Server uses Single-Instance Storage (SIS) to store message attachments. The SIS feature of Exchange permits the Exchange database to only keep a single copy of a message attachment, even if the attachment was sent to multiple users on the same server. NetBackup software uses SIS on the attachments of any types of Exchange data (messages, calendar, Public Folder data, etc.). During the backup of selected mailbox data, NetBackup will only backup attachments once, even though the attachment may be associated with several messages in the selected mailboxes or Public Folder data. In addition to the speed enhancements, less data needs to be transferred and thus less backup media is used.
- **Global Exclude of Deleted and Sent Items** – To further reduce the amount of data backed up, these folders can globally be excluded within a NetBackup policy. It is not necessary for the Exchange backup administrator to configure exclusions for each mailbox separately, saving valuable time during the initial configuration.
- **Configurable Multiplexed and Multistreamed Mailbox backups** – By using the NEW\_STREAM directive within NetBackup software, any combination of data streams can be configured. Multiple streams may be directed to multiple storage devices (i.e. multistreaming) or a single tape or disk device (i.e. multiplexing).
- **Incremental Mailbox-Level Backups** – Both Cumulative Incremental and Differential Incremental backup methods can be used to reduce the amount of data backed up on a given day. NetBackup software tracks changes to mailboxes within Exchange and identifies new email based on the time/date stamps relative to the time/date of the last backup.

When combining these different technologies, mailbox-level backups become a valuable yet manageable complement to your Exchange data protection strategy. The following chart shows the relative improvements to backup times when utilizing single instance storage of attachments, excluding Deleted Items and Sent Items, and

multiplexing several data streams in parallel. Precise improvements to backup times will vary depending upon the amount of attachment data, deleted items, sent items, and processing power available.

## Mailbox-level Backup Time with NetBackup

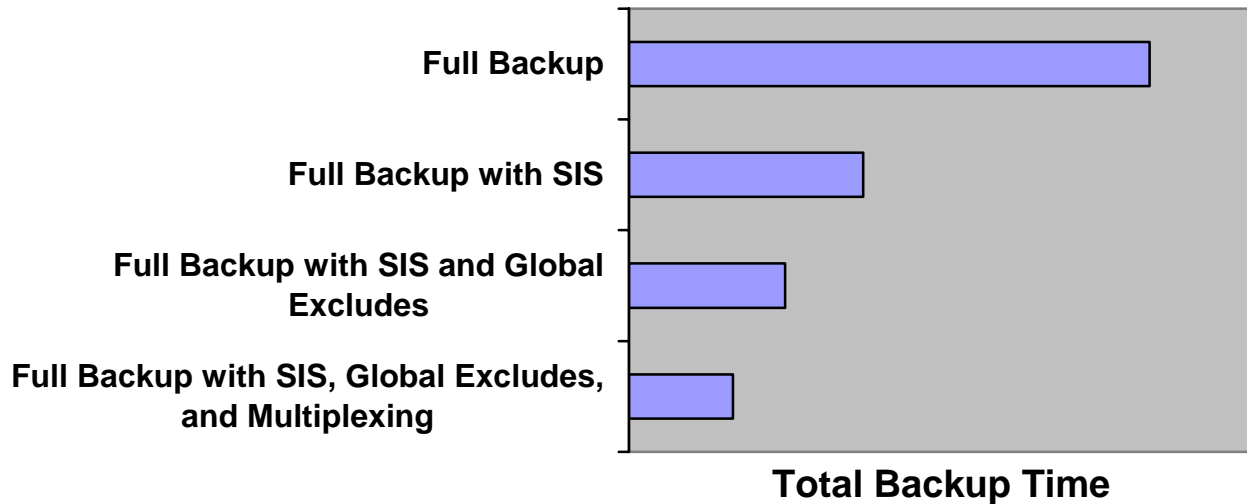


Figure 1: NetBackup for Exchange backup times depending on method used

## OTHER EXCHANGE RELATED SOLUTIONS FROM VERITAS

NetBackup for Microsoft Exchange software is just one of several VERITAS Software solutions which support Microsoft Exchange Server. The array of Exchange Server focused solutions from VERITAS Software may be used separately, or may be coupled together to form a solid foundation for the proactive management of even the most complex and demanding Exchange Server installations. VERITAS solutions that keep Exchange Server highly **available** and **protected** include these products:

- **VERITAS Storage Foundation for Windows** – VERITAS Storage Foundation for Windows software brings advanced volume management technology to Windows Server 2003 and Windows 2000 environments. By creating virtual storage devices from physical disks and disk arrays, Storage Foundation removes the physical limitations of disk storage so you can configure, share and manage storage for optimal results. Compatible with Microsoft Exchange 2003, 2000 and 5.5.
- **VERITAS Backup Exec Agent for Microsoft Exchange Server** – Provides full, online data protection support of Exchange Server databases and components, objects and attributes while also enabling administrators the flexibility to perform individual mailbox backup and restore down to the individual message.
- **VERITAS Enterprise Vault for Microsoft Exchange** - Enterprise Vault is a stand-alone software based solution that integrates with Microsoft Exchange 5.5/2000 and 2003 environments to help you take control over the explosive growth of vital business content found in email. Each Enterprise Vault software component carries distinct advantages to help you meet this goal.

## SUMMARY

Microsoft Exchange Server has quickly risen to the mission critical status in many companies, therefore keeping it highly available and protecting its data is not an option. Like many enterprise database solutions, there are several methods of backing up Exchange Server's data, which can make the administration of the backup process very complex. To tackle this problem, you need to create a data protection plan and select a reliable backup product that suits your environment.

Regardless of the size or complexity of your Exchange Server, **VERITAS NetBackup for Microsoft Exchange** software offers a highly reliable and easy solution to protect your data at either a database level or mailbox level. When disaster strikes, NetBackup for Microsoft Exchange solution can help you to get your Exchange Server back up and running fast. When fast is not fast enough, VERITAS offers several other solutions to keep your Exchange Server available at a higher state as required by your organization.

**VERITAS Software Corporation**  
Corporate Headquarters  
350 Ellis Street  
Mountain View, CA 94043  
650-527-8000 or 866-837-4827

For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at [www.veritas.com](http://www.veritas.com).