VERITAS™ Data Lifecycle Manager

SOFTWARE FOR ENABLING AUTOMATED MANAGEMENT OF DATA FROM CREATION TO DISPOSAL
# TABLE OF CONTENTS

Table of Contents ................................................................................................................................. 2

Data Life Cycle Management .................................................................................................................. 3
  Life Cycle Influences ............................................................................................................................ 3
  Determining Policies ............................................................................................................................. 4
  Compliance ............................................................................................................................................ 4
  Content Index & Search ......................................................................................................................... 5

VERITAS™ Data Lifecycle Manager ......................................................................................................... 5
  Basic Concepts ..................................................................................................................................... 5
  Growth of Data ...................................................................................................................................... 6
  Data Stores ......................................................................................................................................... 6

Data Lifecycle Manager Components ..................................................................................................... 7
  DLM Database ..................................................................................................................................... 7
  DLM Server ......................................................................................................................................... 8
  Quality of Storage Services Option ...................................................................................................... 8
  Content Indexing ................................................................................................................................. 8
  Exchange Agent .................................................................................................................................. 8
  File System Agent ............................................................................................................................... 9
  Administrative Interface ....................................................................................................................... 9
    Data Store Explorer ........................................................................................................................... 10
    Shared Policies .................................................................................................................................. 10
  Extensions .......................................................................................................................................... 11
    Outlook Web Access Extension .......................................................................................................... 11
    Mail Client Extension ......................................................................................................................... 11
    File Retrieval Notification Client .................................................................................................... 11

Data Lifecycle Manager Operations ....................................................................................................... 13
  Data Selection and Relocation .............................................................................................................. 13
  Affinity Groups ................................................................................................................................... 15
  Retention Periods ............................................................................................................................... 15
  Search and Index ................................................................................................................................. 16
  Integration .......................................................................................................................................... 17

Integration ............................................................................................................................................ 17

Summary .............................................................................................................................................. 18
DATA LIFE CYCLE MANAGEMENT

Data life cycle management is a practice aimed at controlling the total cost of ownership for data. This is accomplished by automatically moving data objects to appropriate media as criticality or value changes, and ensuring that data is easily located and used regardless of where it physically resides. The core of this practice is a set of policies that govern how diverse data objects are handled from the time they are created until they are ready to be deleted. The scope of such a practice requires the ability to handle a wide range of data types, operating systems, storage devices, and other infrastructure technology.

Managing data according to life cycles allows organizations to address a number of data management dilemmas.

- Reducing storage costs by pushing data growth to more cost-effective, scalable storage
- Addressing regulatory compliance and corporate governance requirements
- Improving availability and performance by not wasting high-end resources on little accessed data
- Delivering appropriate levels of data protection/disaster recovery
- Alleviating recovery delays due to non-critical data
- Ensuring free space for users and applications

The data life cycle for a 3-tier storage architecture. New and critical data resides on high performance server disk. Lesser used, short-term data is stored on high capacity disk, and long-term, little used data is archived to removable media such as optical or tape.

LIFE CYCLE INFLUENCES

Over the life of a data object, a number of factors will influence how it is handled. Government regulations, user and application service levels, available media, and internal best practices all affect the life cycle of a data object in different and sometimes conflicting ways. Take the example of email. The government may require emails to be kept in an immutable format for 7 years. After which Legal wants it gone forever. Users, of course, want to have it in their mailbox forever; but IT cannot support infinite mailboxes and still meet budget and service-level requirements. IT may prefer to move anything older than 30 days off the server.
A more straightforward influence on data management practices is the available hardware. Many organizations tend to have a wide range of online, near-line, and offline devices. Understanding these resources is key to a DLM practice, making Storage Resource Management (SRM) tools like VERITAS Storage Reporter even more valuable. These tools help make sense of available resources and can help organizations understand what capacities they have at what level of protection, availability, performance, and so on.

**DETERMINING POLICIES**

The results of the data and hardware analyses can then be reconciled with business priorities into policies that will govern how subsets of data will be treated over time. Consider the previous example of email and assume that compliance is the top priority, but does not affect all users. Cost is a close second so IT will have to do this with existing hardware and headcount. Of course, protection and availability cannot be compromised, so in order to keep online data volumes manageable, they can only support 30 days of email in the online messaging environment.

So, in this case a good rule might be something like this: Email is immediately copied to WORM tape. After 30 days, the copy on the server becomes a pointer or stub that is still visible to users via the mailbox, but is actually stored on and referenced from the WORM device for the rest of the 7 year retention, at which time it is deleted. Compliance and legal concerns are met, IT can still reclaim the online space after 30 days. In this case, legal and compliance concerns trump users desires for infinite mailboxes as they need to delete after 7 years. However, for users unaffected by the regulations, IT can support virtually infinite mailboxes for them as only 30 days worth of data is in the message database.

It is this analysis of influences and weighing of priorities that is often the most difficult and time-consuming part of a DLM practice. VERITAS and VERITAS partners also offer services such as the VERITAS Data Lifecycle Assessment to help work through these less-tangible influences and develop appropriate policies. Otherwise, it is advisable to take on one data entity at a time. Perhaps start with email, then file data, then databases, to simplify the process.

**COMPLIANCE**

Compliance is a complex and convoluted landscape with more questions than answers and where change is the only constant. There are tens, of thousands of data management regulations in the world today. Current estimates indicate somewhere around 90,000 unique regulations worldwide. These regulations affect a variety of data (not just email) for public and private companies, in all manner of industries, in virtually every country, state, province, and prefecture.

As such, the tools and practices used to address compliance must be flexible enough to handle a wide range of data and storage types, and they must be open-ended to account for future rule changes or new technology. Point products or solutions that focus on a few data types, operating systems, applications, or storage devices simply will not stand the test of time. The best data life cycle management practices will offer a set of features native to the solution, as well as support APIs or configurations that facilitate interoperability with other applications, platforms, and devices.

Very important, and often overlooked, is the life expectancy of the solution. Some regulations require data to be kept for extremely long periods. Take for example a 30 year mortgage contract. Not only does the data need to be
kept for the life of the contract, but for perhaps an additional 10 years in case of litigation. These solutions must come from vendors who can support their customers 10, 25, 50 years into the future.

**Content Index & Search**

Detailed, documented processes help facilitate compliance, but the reason many of these regulations were put in place is to ensure that the content of that data is available as required. A request for information is likely to center on an individual or group of employees, or around a particular event or project. Simply turning over all data within a given date range could very well result in discovery of unrequested, but nevertheless incriminating data. By incorporating content indexing into a data lifecycle management practices, companies can provide for enterprise wide searches that span a variety of data types. This also allows reviewers to focus on highly relevant data, and not waste time reviewing files or messages with no connection to the issue. This helps ensure that searches are thorough, detailed, and accurate; and reduce the time lost and money spent on the discovery process.

**VERITAS™ DATA LIFECYCLE MANAGER**

Most organizations have far too much data for these practices to be performed manually on an ongoing basis. The volume of data and diversity of storage resources is such that automation is the only way to scale the enforcement of policies. VERITAS™ Data Lifecycle Manager (DLM) is policy-based, data management software that facilitates the creation and enforcement of rules across a diversity of data types and storage devices. Data Lifecycle Manager’s unique integration with Microsoft NTFS, Microsoft Exchange, NetWork Appliance and other environments makes these operations transparent to users and applications. This enables customers to move data to alternate media without affecting user or application workflows, creates a virtual archive across a variety of media types, and makes it transparently accessible to users and applications.

In addition, Data Lifecycle Manager facilitates “e-discovery” with content index and search technology aimed at addressing regulatory compliance and legal concerns. The integration of Autonomy Software's IDOL Engine, allows customers to index DLM managed content and search for desired content. Because DLM can store and index a wide range of data types into a single, virtual archive, customers can dramatically reduce the time and cost of “e-discovery” by performing consolidated searches against a single storage entity.

Integration greatly improves deployment time and overall return on investment in a data life cycle management practice. Application and OS integration means minimal reconfiguration and user training. Integration with high availability and disaster recovery software dramatically improves performance and cost of operations. Unique to VERITAS is the ability to integrate Data Lifecycle Manager with VERITAS NetBackup and VERITAS Backup Exec. This allows VERITAS backup customers to leverage their existing backup storage devices as part of their data life cycle management practice, sharing them with the backup application to increase utilization and provide low-cost, removable media as a storage option for long-term preservation and tracking.

DLM can leverage virtually any disk device, and as mentioned, has the advantage of supporting a wide range of removable media thanks to support for the VERITAS Advanced Device and Media Manager as well as the VERITAS NetBackup Media Manager.*

* Optical media devices including the very latest Ultra Density Optical formats are supported through the Pegasus Disk Technologies InveStore software.

**Basic Concepts**

The basic concepts of Data Lifecycle Manager discussed in this section will help you understand how components work together to archive and manage your data. Data Lifecycle Manager is designed to archive files and messages based on archive and retention policies you set up. This archiving provides a starting point for meeting data retention requirements for regulatory services or internal corporate guidelines.
Archive policies let you control what data is eligible for archiving and define the life cycle of that data. Data is archived into data stores, which are logical groups of media that contain archived data and obtain storage from a media set. A media set is a physical pool of like media that provides media to a data store. Retention policies let you control how long data remains on the primary data source (such as the Exchange store) and how long it remains in the data store. A retention policy acts on a data store.

Growth of Data

The Data Lifecycle Manager Quality of Storage Services Option manages free space on NTFS volumes and Exchange stores. This option will help you to manage the ever-increasing growth of data in your system. There are numerous benefits to implementing space management:

- You can move data into the archive one time and let users or applications access it without moving it back.
- You can store your most frequently accessed data on faster media and your older, less important data on less expensive media.
- To manage free space, Data Lifecycle Manager creates placeholders for files or attachments and stores them in the primary data source and in the data store with the data.

Having placeholders for data means that backup software no longer needs to back up identical data numerous times: after data is in the archive and has a placeholder, the data is safely stored, and only the placeholder on the primary data source needs to be backed up regularly.

Data Stores

Files and messages are archived in logical groups of media called data stores, which are essentially containers for data. Data stores allow data to be organized and grouped into different containers. Different containers can have different attributes. Some may provide different retention practices, some may be regularly indexed to enable easy searches. In addition to data, the data stores keep information about selection rules and actions from policies, and schedules for jobs. All data stores in a media set use the same type of media. Retention policies let you control how long data remains on the primary data source (such as the Exchange store) and how long it remains in the data store. A retention policy acts on a data store.
DATA LIFECYCLE MANAGER COMPONENTS

Data Lifecycle Manager consists of multiple components, as described following this section:

- DLM Database
- DLM Server
- Quality of Storage Services Option
- Content Indexing
- Exchange Agent
- File System Agent
- Administrative Interface
- Extensions

VERITAS Data Lifecycle Manager uses a server-agent architecture to provide flexibility and scalability.

DLM DATABASE

The DLM Database contains configuration-and operation-related metadata that allows Data Lifecycle Manager to archive and retain data. The database runs on Microsoft SQL Server. The server on which the DLM Database resides also stores the database for content indexing. The staging of data for indexing occurs on the DLM Server. Customers can use either standard or Enterprise SQL to suit their needs. The use of popular MS SQL facilitates protection, clustering, replication and other SQL management practices to deliver the desired level of protection and availability of the archive environment.
DLM SERVER

The DLM Server is responsible for the following tasks:

- Storing data that is archived by the Exchange Agent and/or the File System Agent. The media on which the data is stored can be tapes, optical disks, disk devices, and shared network folders.
- Managing data store copies, media copies, and media verification.
- Retrieving freed data from media files if a user or an application tries to open a file or attachment that has been freed using the space management option.
- Consolidating media (on demand or by a schedule), to allow for the most efficient use of media resources.
- Enforcing expiration of data in data stores.

Additional DLM Servers can be installed on machines in your network as needed; each requires its own license.

DLM Servers let you use your existing infrastructure to archive data. You can use the follow types of media and media-management software.

- Tapes on a locally attached or SAN-attached device. Tape media requires the NetBackup, Backup Exec, or RSM media manager. (RSM is the built-in media manager in Windows 2000, XP, and Windows 2003 servers.)
  - Note Data Lifecycle Manager does not take the place of your backup product, nor does it provide a mechanism for protecting its database information. You must use a product such as VERITAS NetBackup or VERITAS Backup Exec to ensure that proper disaster recovery procedures are followed.
- Optical media on a locally attached optical disk changer. Optical media requires either Windows RSM or Pegasus InveStore for media management.

QUALITY OF STORAGE SERVICES OPTION

The Quality of Storage Services Option provides space management for the Exchange Information Store, NTFS volume, or NetApp device by enabling the traditional HSM functionality of Storage Migrator. With the Quality of Storage Services Option customers can create stub files in Exchange, Windows, and NetApp that allow the data to be accessed from alternate storage and moved through a variety of storage media. One Quality of Storage Services Option license will enable this functionality for 10 agents.

Data Lifecycle Manager uses this option to monitor how much space data is using on the primary data source and uses configured policies to determine when to free data from the primary data source, thus making more space available. When the data is freed, Data Lifecycle Manager leaves a placeholder on the volume or Exchange server that allows users or applications to retrieve the data. This option also allows customers to perform multi-stage migrations of data, and implement data life cycle management.

CONTENT INDEXING

Data Lifecycle Manager provides content indexing of data in a data store. After files or messages have been indexed, they can be searched by content and other attributes. Mail messages are indexed based on the content of the message and the content of any attachments. For large data stores, it is most efficient to schedule the Content Indexing job to run at non-peak times.

EXCHANGE AGENT

The Exchange Agent is installed and runs as a service on the Exchange server from which you want to archive messages. The agent keeps track of information such as a message’s sender, recipients, date received, subject, and so on. The Exchange Agent scans Exchange Information Stores and archives all selected messages in a folder.
Data Lifecycle Manager also lets you configure more specific policy rules (based on a message’s Sender, Received Time, Importance, and so on) to let you control the destination data store or retention time for specific messages. For example, you can configure an archive job to archive all data in all users’ inboxes but archive the messages that are of High importance to one data store and all other data to a different data store.

Data Lifecycle Manager keeps a single instance of messages archived in the data store. This means that if a single email is sent to multiple recipients that use the same Exchange database, only one instance (copy) of the message will be added to the same data store.

If you use the space management option (licensed separately), the attachments are archived and and a placeholder is left in the Exchange Information Store. Space management makes Exchange more efficient. Less data in Exchange means less data to be backed up, and, in the event of a disaster, less data to be recovered. As a result, both backups and recoveries are less time consuming and more efficient in using media. A license is required for each Exchange Agent, and an optional license to implement space management is necessary to manage space on each Exchange Server running an agent.

**FILE SYSTEM AGENT**

The File System Agent keeps track of information such as the time since a file was created, modified, or accessed, and properties such as the file name and size. The agent scans data on Windows 2000 (or later) NTFS volumes and archives eligible files to a data store.

To enable File System Agents to archive files, you setup policies that allow Data Lifecycle Manager to select files based on those policies, and archive them to a data store. You can send specific types of data (such as images) to specific media, send older data to specific media, or exclude specific data from archiving.

If you use the space management option (licensed separately), files are archived and a placeholder is left on the managed volume. Data Lifecycle Manager uses that percentage when it sets up and runs an automated Background Space Management job. This detects if free space is low, and if it is, the job deletes files from the primary data source and leaves a placeholder on the file system to allow the agent to retrieve the data if a user or application accesses it.

On a File System Agent with the space management option, you can implement Accelerated Backup. After data is archived, there is no need to continue to back it up: it is permanently backed up in the data store. Data Lifecycle Manager can instruct NetBackup or Backup Exec to backup only the placeholders of freed files. Less data is backed up and less data needs to be recovered. In addition to being faster, backups and recoveries are more efficient in using media. A license is required for each File System Agent, and an optional license to implement space management is necessary to manage space on each file server running an agent.

**ADMINISTRATIVE INTERFACE**

The Administrative Interface is Microsoft® Management Console (MMC) Snap-in used to remotely configure and administer Data Lifecycle Manager components. You use the interface for all of the following tasks:

- To set up agents and policies
- To administer data stores
- To create, run, and schedule jobs
- To monitor DLM activity
- To view, search, and restore files and messages in the data store
- To create shared policies for archiving and retaining data
The Administrative Interface can be installed on any system connected to the server running the DLM Database. Note To administer media and perform device-related management; use the NetBackup, Backup Exec, or RSM administrative interface (console).

The Administrative Interface has two panes: a Scope Pane and a Results Pane. When you open the interface, the Scope Pane lists the first-level components (in a tree structure) and the Results Pane provides a brief Description of them.

Data Store Explorer

The Data Store Explorer provides a view into data stores, and both search and restore capabilities for archived files and messages. It lists objects in the archive, and you can mark specific files or messages and restore them to a volume on a server running a File System Agent or to an Exchange store on a server running an Exchange Agent. You can access the Data Store Explorer by right-clicking a data store and selecting Explore Contents.

Shared Policies

Shared policies contain data selection rules that can be used by multiple File System Agent jobs or multiple Exchange Agent jobs to control how data is archived. (You can also create private policies that are visible only to one job.) A shared policy can be used across any number of machines without modifying the individual configuration on those machines.
You can configure data selection based on criteria such as time since creation, modification, or access; message recipients or senders, and other properties such as whether a file is a system file.

Rules can include or exclude files or messages from archiving, based on criteria such as the volume on which data resides, file names or types, recipients, senders, and so on.

Rules are associated with actions that will do such things as archive or retain selected data.

Templates of shared or private policies are provided for ease of implementation.

For example, the Retention Template for Retention policies specifies freeing data after 90 days, removing it from the primary data source after one year, and then expiring it in the data store after three years. Templates are different than actual policies in that the template is never associated with a data store and therefore cannot cause data to be archived.

EXTENSIONS

Data Lifecycle Manager provides extensions for licensed features.

- The Outlook Web Access Extension is required for OWA users to access freed attachments. It is installed and runs on the Exchange server.

Extensions

- The Mail Client Extension is required for Outlook users to access freed attachments. It is installed and runs on the user’s client system.
- The File Retrieval Notification Client provides status information during retrievals. It is installed and runs on the user’s client system.
- The Windows Explorer Extension controls user archiving of files and freeing space on volumes. It is installed and runs on the user’s client system.

Outlook Web Access Extension

Data Lifecycle Manager supports Outlook Web Access (OWA) on Exchange 5.5, Exchange 2000, and Exchange 2003. The OWA Extension allows access to free attachment data. You must install the OWA Extension on the Exchange server. It has a separate installation from the other extensions, which are all installed on clients. OWA users do not need to have the Mail Client Extension installed to access freed attachments.

Mail Client Extension

The Mail Client Extension (MCE) is a part of the space management option for Exchange users. It accesses the data from freed attachments on a managed Exchange server. You use can use either the Client Extension installation or Microsoft MSI to install MCE on all desktop systems that use the Microsoft Outlook client. If you have installed the OWA Extension on the Exchange server, users running Outlook Web Access can access freed attachment data without the MCE.

With MCE installed, a user accesses a freed attachment in the usual manner, the data is retrieved from the data store, and the file is opened on the user’s desktop. The user sees a message indicating that the attachment is being retrieved from the data store.

File Retrieval Notification Client

The File Retrieval Notification Client notifies users when a retrieval of a freed file is taking place. It is not necessary to have the extension installed in order to retrieve a freed file.
The client provides additional functionality when users retrieve files:

- A Cancel button gives users control over whether they want to wait for the file to be retrieved
- A checkbox lets users choose to put the file in a queue to be retrieved the next time the retrieval queue is processed
- A message unique to Data Lifecycle Manager allows users to know more specifically what is happening to their files

After a file is freed, its icon is changed: a small black clock is added to the lower left corner. Users access freed files as usual, and if the File Retrieval Notification Client is installed, a message informs them that the data is being retrieved from the data store. On Windows 2000, Windows XP, and Windows 2003 systems, users receive a default retrieval message from Windows, but installing the File Retrieval Notification Client is still recommended. On Windows NT clients, users receive a message only if you install the File Retrieval Notification Client.
DATA LIFECYCLE MANAGER OPERATIONS

Data Lifecycle Manager operations are relatively straightforward. Administrators build sets of rules to create policies that are applied according to schedules, in specific events, or manually as needed. These policies are configured at the DLM Server through the DLM Administrative Interface. These policies can be applied to file systems, messaging environments, and storage devices. Policies are enacted through jobs. Jobs are collections of policies that are run at the same time. During a job, DLM Servers communicate with DLM Agents to scan data objects for the desired criteria. Selected data objects are then handled as dictated in the policy.

DATA SELECTION AND RELOCATION

Though selection criteria will differ widely depending on the environment, there are some common traits that can be used in many environments, such as:

1. Who owns, created, last touched the data
2. What file names, file types need to be selected
3. Where to look for the data (folder, mailbox, machine)
4. When was the data created, modified, accessed
5. How important or sensitive is the data

Once the selection criteria has been entered, the next step is to decide what to do with that data. Data Lifecycle Manager offers a number of options.

- Copy to alternate media
  - Fast, online access to data
  - Data is still in its original location
- Data copied to archival or compliant media
  - Disk, tape, and optical
- Streamlined NetBackup and Backup Exec operations
  - Backup and restore operations complete more quickly and use fewer medium because NetBackup and Backup Exec are “aware” of DLM copies.
- Rapid availability of free space if needed
  - If free space drops below a configured percentage on primary storage, DLM can immediately truncate the object to free up space.
- Example: Tape based Microsoft Exchange compliance archiving. Data remains on the server to meet SLA for email, data copied to tape for long-term, compliant retention.

- Copy and truncate
  - Transparent access to data for users and applications via placeholder or “stub” file
  - Immediate availability of free space upon copy verification

- Streamlined operations for any Windows certified data protection solution
  - Microsoft integration allows Windows certified backup and anti-virus operations to properly handle DLM placeholders.
- Example: Tiered storage for a variety of NTFS data.
  - Objects on front-end servers that have not been modified in 90 days move to near-line disk. Data on near-line disk that is not accessed for 1 year moves to tape. If not accessed from tape for 3 years, data is deleted.
  - Placeholders provide users and applications access to the latest version of data regardless of where it is moved.

- Copy and remove
  - Copy to alternate media and delete the original
  - Immediate availability of free space upon copy verification
  - Removed data objects no longer impact protection/recovery times
  - Example: ISO or FDA process documentation. Old versions must be retained, but must not be available to prevent confusion.
Data staging options: A) Unmanaged, B) Copy to alternate media, C) Copy and truncate, D) Copy and remove

AFFINITY GROUPS

Data Lifecycle Manager lets you organize the data that has been archived or data to be reorganized, you must associate it with a grouping key in a policy. After you run a reorganize data job, files that are associated with the same grouping key are located as close together on media as Data Lifecycle Manager is able to locate them. Each rule in a policy can have its own grouping key, which means that one job may assign many different keys.

Reorganizing data into groups helps reduce the number of media mounts required to retrieve it. By minimizing media mounts, you reduce the time it takes to retrieve data. For example, if the data you want to retrieve is placed in the data store based on when it was copied, retrieving it might mean that Data Lifecycle Manager would need to request six tapes to be mounted. If it were grouped together on media, only one tape mount may be needed.

RETENTION PERIODS

To ensure that data is retained in the Data Lifecycle Manager system, you create Retention policies that support your needs. After a configured time has elapsed, media holding expired data is available for reclamation during the data consolidation process. You apply Retention policies at the data-store level. Data is eligible to be deleted in the data store only after it has expired and has been deleted from the primary data source (that is, no copies of it exist and no placeholders exist). The data is removed from the data store when a data store consolidation job runs.
Retention policies are not created as a subset of an archiving policy; they are created separately using the Retention Policy Wizard. A retention policy can be associated with an archiving policy so that data selected by specific rules is retained based on its selection criteria.

For example, if all *.gif files are selected by a rule, they can be retained on the primary data source for one year and then deleted and exist only in the archive. If all *.jpg are selected by a different rule, they could be freed from the primary data source immediately, and then be expired in the data store after three years.

Retention policies control the management of data over time by carrying out specified actions based on various time stamps or data usage. Actions include data relocation, file truncation, removal of active or archive copies, etc.

SEARCH AND INDEX

Data Lifecycle Manager can index the content of files and messages in data stores in the archive. After files and messages have been indexed, you can search for words or phrases in the text, or for other attributes such as a message recipient or file type. One of the major advantages of the DLM Content Index is that it provides administrators with search tools that span a variety of data types and storage media. This dramatically reduces
the time and cost of e-discovery. "E-discovery" refers to the location and retrieval of desired data objects. Whether it is locating a file for a user, or tracking down a number of related content for a legal issue or compliance audit, a single, consolidate tool can save a significant amount of time and money.

Once the index is created for a given data store, searches can be conducted to locate email, attachment, file, and any other data in the indexed data store. Words or phrases, file names, file types, dates, user IDs, and file size are just some of the available criteria. Administrators can also browse data by which device it came from, and the media upon which it now resides.

Search criteria include words or phrases within a data object, file names, file type, messages, attachments, date ranges, and even user IDs. Results are presented with relevancy scores and can be restored to file systems, messaging environments, or removable media.

Data can also be browsed by where the data originated and where it is currently stored.
INTEGRATION

Unmatched integration with VERITAS NetBackup™ and VERITAS Backup Exec™ enables Data Lifecycle Manager to leverage existing backup hardware, extending data protection investments to address compliance, improve backup/restore times, and enable long-term data retention. In addition, the integration allows customers to apply Data Lifecycle Manager features to existing backup media, indexing their existing backup media for easier restore selection and applying retroactive archive and retention policies.

Integration also enables Data Lifecycle Manager to leverage NetBackup and Backup Exec media, dramatically reducing the cost and complexity of deployment. VERITAS Desktop and Laptop Option (DLO) for NetBackup and Backup Exec further extends Data Lifecycle Manager functionality to end user desktop data (files messages and message archives), helping IT gain control over all data. The software is also compatible with other infrastructure applications such as VERITAS Cluster Server, Microsoft Cluster Server, and VERITAS Volume Replicator to support high availability needs.

Data profiling and storage resource management are critical to the planning and feedback process for a data lifecycle management practice. Regular review of usage patterns and value of data, combined with oversight and mapping of storage resources provides the input needed to create and update DLM policies. When used in conjunction with VERITAS CommandCentral Service, VERITAS SANPoint Control and VERITAS Storage Central, Data Lifecycle Manager helps address a whole host of other pressing IT concerns including storage utilization and efficiency, system performance, and delivering storage as a utility.

VERITAS Data Lifecycle Manager also supports a variety configurations and API integrations of third-party hardware and software, allowing DLM to serve as a core archiving tool that manages diverse data types across a wide range of different hardware. This enables VERITAS Data Lifecycle Manager to service environments for which VERITAS has not yet developed specific agent technology. This also allows 3rd party applications to access a virtual archive that spans a variety of media. Current partnerships through the VERITAS Enabled program allow Data Lifecycle Manager to handle instant messaging, voice mail, database archiving, enterprise content management, and a host of other data types. VERITAS Enabled hardware partners allow Data Lifecycle Manager to talk to WORM disk devices and optical storage.

SUMMARY

VERITAS Data Lifecycle Manager provides customers with a centralized, policy-based data management tool. By integrating archiving, hierarchical storage management, and content search and index, VERITAS delivers a unique solution for controlling the total cost of ownership for data, facilitating regulatory compliance, and reducing the cost of “e-discovery.” VERITAS Data Lifecycle Manager uses agents for Microsoft NTFS, Microsoft Exchange Server, and NetWork Appliance devices, in conjunction with an array of API and configuration partners to manage a wide range of data types into a shared, virtual archive that spans diverse media types. When used in NetBackup or Backup Exec environments, DLM shares licensed backup storage resources thereby extending investments in data protection hardware and software. This common storage infrastructure improves hardware utilization, streamlines backup and restore operations, leverages existing IT skills, and enables content indexing of backup data. For these reasons, and many more, VERITAS Data Lifecycle Manager is the answer to a variety of data dilemmas.

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.