



IT Knowledge • Business Results

# Market Review

Unlocking the True Power of Enterprise Message Management -

*Beyond Tactical Email Archiving Towards a Strategic*

*Comprehensive Information Governance Infrastructure*

By Steve Duplessie, Senior Analyst  
Peter A. Gerr, Senior Analyst  
Data Management and Data Protection Solutions

September 2005

Table of Contents

**Introduction**..... 2  
    Enterprise Message Management - The New Mission Critical Application ..... 2  
**Enterprise Messaging - A Classic IT Challenge Morphs into a Business Risk** ..... 3  
    IT & Business Professionals Must Quantify RTOs and RPOs ..... 4  
    The New Information Stewards - Compliance, Legal, Risk, and Information Security..... 4  
**Building a Cost /Benefit Case for EMM and CAS**..... 6  
    How EMM and CAS Reduce IT and Business Costs ..... 6  
**Conclusion** ..... 10

## Introduction

### Enterprise Message Management - The New Mission Critical Application

It's a scenario that is increasingly all-too-familiar among enterprises as well as among the tens of millions of small-to-medium businesses around the globe: The data center phone rings. On the other end, a frantic Executive is demanding immediate access to all his/her emails - and their attachments - that contain certain keywords and involve certain individuals for the past 12 months. *"It's a matter of life and death,"* is the directive as the phone slams down. Or perhaps it's the VP of Human Resources requesting all emails and personal electronic files from a recently terminated, long-time employee who is threatening a lawsuit. The employee's records are scattered across the employee's laptop and hundreds or thousands of backup tapes, some of which are stored at an offsite facility while others are haphazardly organized in the back office of the data center or in a filing cabinet.

#### WHY FOCUS ON ENTERPRISE MESSAGE MANAGEMENT?

- ✓ Enterprise Messaging applications have become mission critical to modern business
- ✓ "The Smoking Gun" problem -Electronic communications & records heavily scrutinized, now considered an "evidentiary business record"
- ✓ Enterprise messaging, management & archival (EMM), though vital, is not a core competency
- ✓ EMM solutions can:
  - o Deliver operational & administrative efficiencies
  - o Mitigate risk associated with enabling CG / compliance
  - o Help transform technology-driven lifecycle management of EM into business-aware, intelligent management additional content / data types and classes
- ✓ **THE BOTTOM LINE** -
  - o EMM solutions transform risk / liability into strength / asset

While this scenario may seem simple enough to the casual bystander or even the Executive making the request, the reality of the task and the shortcomings of most user's information recovery processes can incite a chain of panic among even the most-experienced IT departments today, and for good reason. The truth is that traditional email management and backup procedures have not improved and evolved at the pace of business. Over the past few years, email repositories (i.e., Exchange and Notes servers) have grown exponentially in both size *and* in strategic importance to the entire organization.

According to a recent survey conducted by the Enterprise Strategy Group (ESG), email/messaging is the number-one data-protection concern among IT departments today, ahead of OLTP/OLAP/RDBMS, financials, business intelligence/data warehousing, and CRM applications [see **Figure 1: Why focus on Enterprise Message Management**].

Email and other forms of electronic communications are unique applications, in that, they are typically used by every employee of an organizations regardless of functional role, and for most individual contributors / knowledge workers, their email client is the universal portal through which the vast majority of their daily work passes.

However, while the majority of organizations today recognize the strategic importance of email applications, notably Microsoft Exchange, few have actually taken advantage of new email messaging management and

archiving (EMM) solutions (e.g., Symantec Enterprise Vault) and innovative content-addressable storage (CAS) technologies (e.g., EMC's Centera) to ensure that email message content (semi-structured data), metadata, and associated attachments (unstructured data) - the workflow of daily corporate life - is readily available for recovery. Whether IT needs to recover a complete Exchange Storage Group after a system crash; an Executive or Board member must retrieve a single, but invaluable, email; or the Chief Compliance Officer must perform an audit to meet regulatory and corporate governance requirements, the combination of an enterprise message management software solution coupled with a content-addressable storage system is perhaps one of the most valuable and cost-effective means to achieving information governance initiatives involving email today.

## Enterprise Messaging – A Classic IT Challenge Morphs into a Business Risk

A major by-product of the “Internet Boom” is that our global economy and most businesses from Wal-Mart to the most recently-funded startup relies on the creation, protection, preservation, and sharing of information - in short, information is the new global currency and perhaps the most valuable of all corporate assets. And like any asset, there are federal, state, industry-or-corporation-specific rules to protect information and communication channels from misuse and abuse. These new rules of information governance and regulatory compliance demand a new way of implementing an effective data protection strategy. IT departments today need EMM solutions that not only meet today’s email message requirements but are scalable and flexible enough to meet tomorrow’s mandates.

In fact, most organizations today still rely on tape-based archives to protect their Exchange assets; IT departments generally back up Exchange servers to tape (e.g., SDLT, LTO, etc.) periodically, and then move these tapes offsite for disaster-recovery purposes. While a tape-based backup offers a gross-level approach to email/data protection, backups alone do not provide the ability to quickly pinpoint and respond to a compliance or legal event involving email, and this is a critical risk.

At a minimum, the consequences of not being able to quickly locate, search, and restore email from tape (a sequential-access versus random-access device) can be costly, considering it can take days, weeks, or even months to process and restore email from tape. When compared to even the most basic disk-based device, finding and retrieving data from tapes is a time-intensive and costly process. In many cases, when historical or archived data needs to be retrieved, IT must go through the tedious process of rifling through huge stockpiles of tape cartridges before finding the right tapes and then streaming data off the tape through the application server (at tape speeds) for the restore process. That is, of course, if the data being requested was backed up properly or at all, is resident in a readable format on the tape in question, which itself could be compromised from old age.

As a gauge, ESG estimates that it costs an internal IT department between \$1,500 and \$3,000 to process and restore a single backup tape; IT would pay approximately the same rate if the organization has outsourced its long-term archiving or disaster recovery processes to a 3<sup>rd</sup> party service provider and must initiate a recovery operation to retrieve the data. In the most extreme case when the organization is under a deadline-driven compliance audit or electronic data discovery (EDD) in order to respond to a litigious claim, IT can expect to pay 2-3 times as much to process a single tape. Perhaps the old adage, “*time is money*”, should be rewritten for the 21<sup>st</sup> century as “*timely access to information is money*”.

When ESG compared the hard (tangible) and soft (intangible) costs of recovering archived email from within a tape-based archive with that from within an integrated disk-based email management and archiving solution, such as EMC’s Centera with Symantec’s Enterprise Vault, the differences are dramatic. ESG research indicates

### WHAT’S AT STAKE?

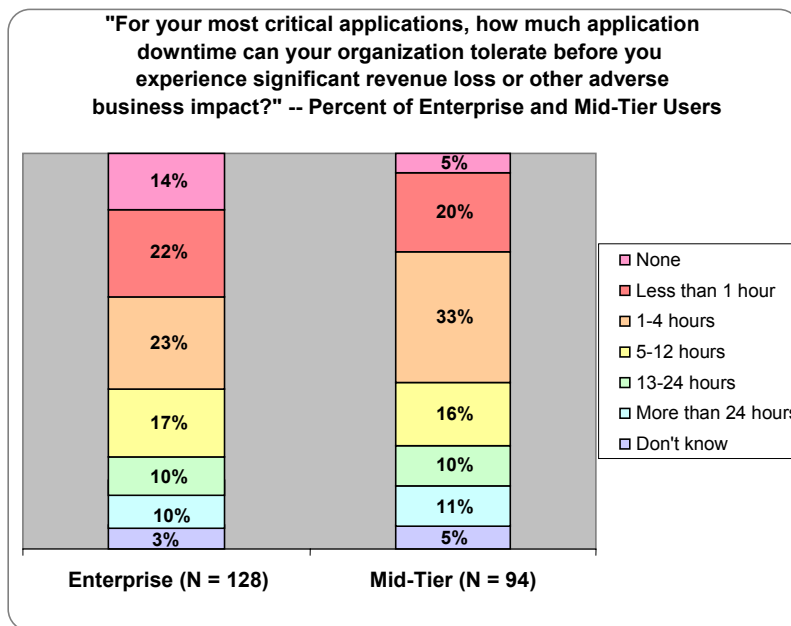
- 2001 - Enron Corp. and Arthur Andersen LLP - Andersen’s corporately-sanctioned document retention policy allowed for destroying “unneeded” files just as the SEC began looking into Enron’s finances. Andersen was forced to surrender its accounting license after being convicted of destroying documents (case currently in appeal) and was later required to pay more than \$60 million to settle civil lawsuits.
- 2004 - Phillip Morris USA Inc. - sanctioned \$2.75 million after it was ruled that 11 employees failed to preserve emails, as was required by the company’s retention policy and the court’s preservation order.
- 2005 - Morgan Stanley - found “grossly negligent” by a Florida state judge in failing to produce emails and other documents related to Sunbeam Corp. in response to financier Ronald Perelman’s \$2.7 billion lawsuit.
- 2005 - Bank of America - admits that it has lost backup tapes that contained personal information including Social Security Numbers and account information for some 1.2 million federal employees. At the time of this paper’s publishing, this incident was still under investigation.

that organizations can realize over \$800,000 in benefits when deploying an integrated message archival system. These benefits range from avoiding compliance related fines to improving utilization of storage resources that support the archive.<sup>1</sup>

**IT & Business Professionals Must Quantify RTOs and RPOs**

When a mission-critical application like email goes down, the entire business is adversely affected - remember that old (new) adage. The sheer impact to internal and external corporate communications is perhaps the most benign penalty. Enterprise messaging applications, like email, are integral parts of enterprise business applications (EBA), such as sales force automation (SFA), customer-relationship management (CRM), and enterprise resource planning (ERP) suites - these truly form the foundation of the business. Beyond the direct value to information governance and storage capacity optimization from implementing an EMM solution, simply migrating a corporate email archive from a tape-based solution to a disk-based solution can greatly accelerate recovery performance - reducing both costs and risks to the business. In a recent ESG Research study, 59% of enterprise and 58% of mid-tier respondents stated they would experience significant revenue loss or other adverse business effects if their most-critical applications (e.g., email) were down for four hours or less. Clearly, the ability to quickly retrieve emails and associated attachments can have far-reaching business benefits [see

**Figure 2: RTOs are increasingly stringent].**



Due to the sheer volume of email messages being created daily and the limitations of tape-based backup infrastructures (e.g., the backup window isn't big enough to back up the Exchange database nightly), many IT departments today have been forced to impose capacity quotas that put business users in the unenviable, and potentially unlawful, position of managing, and, yes, deleting, crucial email - email that may ultimately be critical in mitigating risk in either corporate governance or regulatory compliance situations. This is a business practice that should evolve or change in order to mitigate the risk of an audit. It is becoming apparent that those who knowingly delete emails with intent to potentially impede a future investigation - could find themselves in

jail, per Section 802 of the Sarbanes-Oxley Act. This, and other impending legislation, should be enough to bring everyone into the fold around an Enterprise Messaging strategy and corporate best practice. This will not be restricted to the large, public entities - but all companies, and eventually, all individuals.

**The New Information Stewards - Compliance, Legal, Risk, and Information Security**

With no end in sight to data growth, ESG believes that IT and business professionals in a variety of industries, will continue to earnestly evaluate EMM solutions such as Symantec Enterprise Vault as well as purpose-built CAS storage solutions like EMC's Centera Governance Edition. While the value of EMM and CAS solutions are well-understood by general IT professionals, storage managers, and email administrators, the fact that EMM and CAS solutions are an effective means to mitigate some of the legal and regulatory risks inherent in electronic communications will increasingly draw legal, compliance, risk management, and audit professionals into the conversation. If information technology and IT professionals represent the plumbing and plumbers of an organization, respectively, their role is fairly straightforward - keep the pipes clean, keep the asset/resource, in this case information not water, flowing. Oh, and by the way, protect the source. Continuing the analogy,

<sup>1</sup> Reference - ESG's Enterprise Message Management and Archiving Cost-Benefit Tool, 2005

compliance, legal, and risk management professionals assume a critical role - to protect, secure, and preserve the assets for some period and ensure that the organization can reconstruct an electronic “chain of custody” - an immutable chronology of every action performed throughout the lifecycle of each unique information object (file) created, preserved, or eventually, disposed of.

Many of the recent incidents involving the loss, theft, or misplacement of unencrypted backup tapes while in transit serve to underscore the potent threat facing corporations, and by extension, shareholders today. Conversations with Executives, IT, and Legal professionals lead us to conclude that as much as 75% of corporate intellectual property (IP) is accessible either directly or indirectly via email and other messaging applications<sup>2</sup> within the typical commercial enterprise, SMB, or government, and academic organization. The most troubling prospect, therefore, is that the very same corporate IP that resides on those lost backup tapes contains private, sensitive, or otherwise confidential information. While the financial services, broker-dealer, insurance, and broad financial markets have born the brunt of the compliance and regulatory backlash over the past 5 years, other industries will soon have to choose whether to address EMM and all its associated challenges proactively or reactively (hint: the latter is very, very costly). Simply stated, it's not a matter of if, but rather, when incidents like the ones described above occur within a healthcare organization, hospital, or HMO, or perhaps the entire student body history of a state's public school system will be breached or hacked and exploited for malicious purposes. While a recent ESG Research survey showed that only 7% of organizations consistently encrypt their backup or archival data sets<sup>3</sup>, ESG believes that encryption and other proprietary means of securing the privacy of data in transit, but more importantly, at rest will become a “must-have” for compliance, legal, and risk management initiatives.

In fact, EMC's Centera is one such system that has fundamentally altered the ways in which people store, access, and preserve the integrity of information. Centera stores information in randomly sized sub-file sized objects, each of which are individually identified by a unique digital ID or fingerprint, the metadata of which describes the data object itself. Symantec Enterprise Vault extends the capability by creating a Centera object for attachments such that files can be de-duplicated even when attached to different messages - such as the corporate PowerPoint document that is circulated repeatedly. A combined solution with Centera and Enterprise Vault can form the foundation of a comprehensive, secure, scalable, and sustainable information governance initiative and ensure IT, Business, and Information Governance professionals are ready to defend their castle and its jewels from those who would do them harm (not to mention the very straightforward cost/benefit and ROI of implementing such a solution!)

---

<sup>2</sup> Reference – ESG Viewpoint, 2004

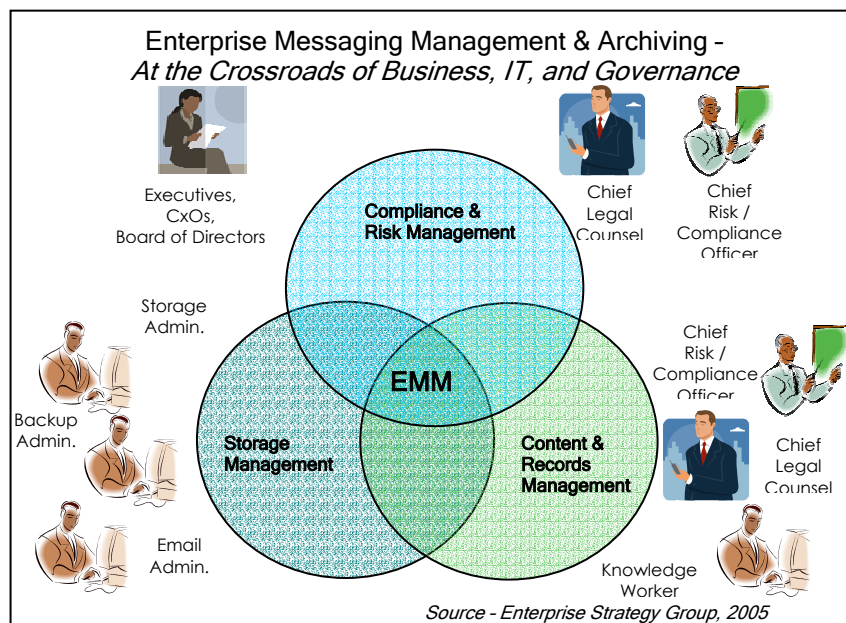
<sup>3</sup> Reference ESG Research report – “Information at Risk – The Troubling State of Backup Encryption, April 2005

## Building a Cost /Benefit Case for EMM and CAS

### How EMM and CAS Reduce IT and Business Costs

In fact, ESG research shows that implementing an email archiving solution, such as Symantec Enterprise Vault, with a content-addressable storage (CAS) platform, such as EMC Centera, can extend the life of the typical email server by shifting the burden of primary email storage from the email server to the CAS repository, which has been designed from the ground up for fixed-content data, such as email, attachments, instant messages, etc. Users also report significant cost- and time savings as a direct result of the shortened search and discovery process that is possible with this type of EMM implementation.

Chances are you're not prepared to handle CxO requests, you are not sure how compliant your organization's email applications are, the thought of extracting business value from your email is still nothing more than a pipe-dream, and you're email spending is out of whack. Before you throw your hands up in despair, remember you're not alone.



EMM, or the process of applying traditional (paper-based) records retention management processes to the digital world without compromising business productivity, is still in its infancy. In fact, most organizations today, except for those in heavily regulated industries such as financials, government, etc., still treat EMM as an event- or cost-driven tactical undertaking rather than a "core" competency. In other words, they deal with email management issues on the fly as events unfold or as dollars become available. This type of view is shortsighted.

EMM represents the nexus of storage management, content and records management, and compliance and risk management [see **Figure: EMM:**

**At the crossroad of IT & Business].** In combination, these tools can help organizations:

- ✓ **Reduce** email-related capital and operating expenses (CAPEX and OPEX)
  - Minimize email volumes (the reduction of the number of duplicate copies of email messages and attachments)
  - Extending the life of storage/server resources, and archiving email to lower-cost (e.g., SATA) media
- ✓ **Improve** email application performance and availability
  - Reduce backup windows and messaging server performance issues associated with large information stores
- ✓ **Mitigate** some of the risks associated with regulatory compliance and corporate governance (e.g., hefty fines or penalties for delays in recovering email content);
- ✓ **Prevent** issues of data corruption and loss related to end-user ad-hoc archives (e.g., PST files in Microsoft Outlook);

- ✓ *Reduce* costs for legal discovery and monitoring
  - Eliminate reliance on expensive third-party services or internal processes around data restoration from tape;
- ✓ *Increase* productivity and administrator efficiency
  - Enable IT administrators and users faster access to email contents according to pre-determined recovery time objectives (RTOs)
  - Eliminate the need for email quotas and reducing administrative/support staff needed to support the application.

While regulatory compliance has lately received a lot of press - particularly, in heavily regulated financial and healthcare industries - corporate governance has been steadily inching its way up the IT importance meter, largely due to recent publicity surrounding Enron and WorldCom. It is expected to influence IT purchase decisions going forward.

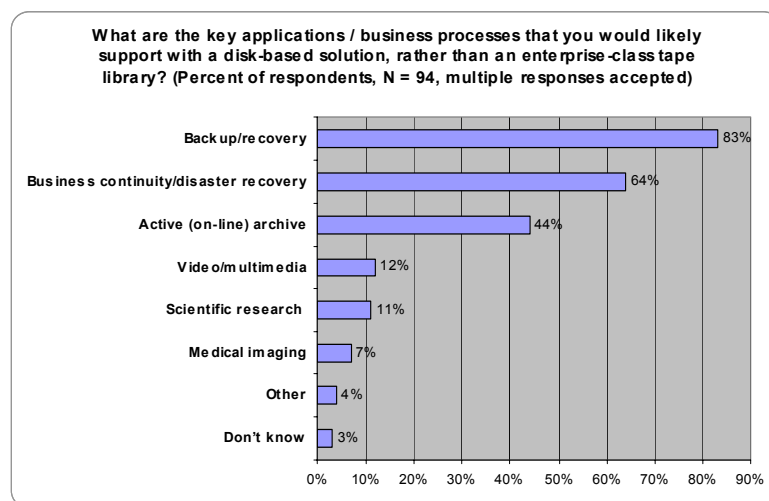
Whether we like it or not, email has become the communications “hub” for most organizations; it is the vehicle by which most corporate intellectual property (IP) is now shared, distributed, stored, and accessed. The challenge before IT departments today is how to protect this hub, while taking full advantage of the content/information (i.e., intellectual property) that travels through it.

From a corporate governance standpoint, EMM tools can help organizations: (1) reduce the cost and time it takes to support litigation and perform electronic discovery; (2) enable proactive sampling, supervision, and electronic discovery; (3) automate archiving, retention, and deletion of messages according to set policies; (4) provide a single point of control for corporate IP (e.g., email content); and (5) reduce the risk or/discourage unlawful or illegal conduct by employees, among other things. These benefits mitigate the risk associated with litigation, lower the associated discovery costs, and protect valuable intellectual property.

*Litigation and discovery.* This is a growing concern among most organizations. While virtually any size public or private organization is at risk, insurance, healthcare, consumer products, financial services, and pharmaceutical companies are often under the greatest scrutiny. Organizations need to ensure that archived emails and other content are not only readily accessible but also continue to meet RTO objectives. Potential implications of a “flawed” litigation and discovery process include fines and sanctions, loss of shareholder value and trust, class action lawsuits, criminal charges, and prison terms for executives.

*Corporate IP.* First and foremost, IT administrators are responsible for managing and preserving corporate IP and ensuring that electronic business records comply with corporate and regulatory compliance guidelines. Beyond that, IT departments will be asked to look at email content from an “information-centric” perspective to not only ensure that the appropriate level of protection is applied to the email so that it is ultimately stored on the right-cost media (see bullet below), but also to begin to bring email into the overall business workflow process. This requires strong content and records management capabilities.

#### Disk-based Solutions Address Tactical (Backup/Recovery) & Strategic (Active Archiving) Objectives



Source - Enterprise Strategy Group, 2003

### EMC Centera and Symantec Enterprise Vault - Pushing Information Governance Forward

New rules demand a new way of doing things. IT departments today need EMM solutions that not only meet today's email message requirements but are also scalable and flexible enough to meet tomorrow's standards.

EMC and Symantec have teamed up to provide a complete EMM business solution for both enterprise and medium-sized organizations. Symantec Enterprise Vault was one of the first products to integrate with the Centera platform and API through EMC's Centera Partner Program.

Symantec Enterprise Vault 6.0 serves as the central archive to index and secure information from the front-end messaging systems and other information repositories. Enterprise Vault is integrated with EMC Centera CAS system, which serves as the "physical store" for the email implementation. This integration includes Enterprise Vault's ability to migrate double-byte characters stored within the Centera. Other notable Enterprise Vault features include a Compliance Accelerator, as well as a Discovery Accelerator. The Compliance Accelerator allows supervisory review of electronic communications (i.e., monitoring or surveillance) to comply with NASD regulations or to enforce internal policies (e.g., around profanity or intellectual property distribution). Discovery Accelerator is designed to facilitate and audit the internal workflow of running searches, marking records and producing items (in formats courts or third-party counsels can consume) for legal discovery situations. The combined solution ensures integrity of email messages and complete audit logging.

#### EMM and Archiving Drives IT and Business Benefits

- ✓ Executive Management, CxOs, Legal & Compliance -
  - Enables organization to proactively reduce corporate risk & lower IT costs
  - Improve organization's ability to manage & protect corporate IP
- ✓ IT, Storage, Network & Server Administration -
  - Replace ineffective, costly, & risky EM management practices
  - Extend life of server / storage assets while improving EM performance
  - Improve / maintain data protection levels as EM volume grows
- ✓ Knowledge workers, Staff -
  - Increased productivity, reduction / elimination of PSTs & quotas
  - Minimal impact to workflow with short learning curve

SOURCE: ENTERPRISE STRATEGY GROUP, 2005

EMC's Centera CentraStar software assigns a unique content address, based on its content, for each email message or attachment generated by Exchange and then "clips" key metadata to the content address for identification purposes and then hands a secure "C-clip" back to Symantec Enterprise Vault. From that point on, all email management requests (e.g., searches, retrievals, etc.) are done via the Enterprise Vault (including Compliance or Discovery Accelerator). All interaction between the two platforms is completely transparent to the user. Restoring email from the Centera archive is done via Enterprise Vault, using Outlook shortcuts stored in the mailbox, or the tool's web-based Archive Explorer

interface. Email content is recovered directly from the Centera archive at ATA disk speeds (Centera uses ATA disk drives); no tapes are used. The system scales to billions of objects and is high performance in both archiving and search/retrieval.

It is also worth noting that Enterprise Vault can also be used with other EMC platforms, including Symmetrix, CLARiiON ATA disk, and NS Series and Celerra NAS platforms.

Enterprise Vault's Archive Explorer feature allows users to organize archived C-clips by type (e.g., email, document, instant message, etc.), subject, date, or other criteria. Groupings are presented in a Windows-Explorer-like hierarchical folder structure, which can be then searched using an embedded Alta Vista tool. Users can do a search of the full index (including attachments), the metadata alone, or the metadata and some amount of discrete partial phrases.

Additionally, Enterprise Vault optimizes storage usage with EMC Centera in several ways. First, it separates messages from attachments and hands each attachment and the original message to Centera separately. This allows Centera's single instance storage feature to work across the same attachment found in different (e.g., forwarded) messages - or even between an attachment in an email and the same file found in a file system archived by Enterprise Vault File System Archiving. Second, it optimizes the number of objects in Centera (to maintain optimal performance) by collecting small items together and handing "containers" to Centera. Further, the joint solution can help facilitate customer requirements around data resiliency. Enterprise Vault can ensure that Centera has replicated an archived item, before it is removed from the primary system (e.g., Microsoft Exchange). This allows IT organizations which operate under rules where two copies of data are mandatory, to ensure that this is always the case.

The latest release of the product - version 6.0 - includes support for additional sources of archived content - Lotus Domino Journaling (available in SP1 -- Fall 2005); SMTP message capture; and Microsoft SharePoint™ Portal Server 2003. It also offers automated discovery, management and migration of PST files, and new "intelligent" archiving capabilities. The new intelligent archiving capabilities include the ability to "filter" incoming data, "categorize" archived data for better retention and retrieval; and specialized tools for compliance and E-discovery. Additionally, Enterprise Vault integrates with Symantec NetBackup, and provides enhanced Centera support. This includes the ability to "map" Centera Retention Classes to Enterprise Vault Retention Categories, for granular control over item retention and expiration.

These enhancements, in combination with the Centera platform, are expected to further improve a users' EMM experience, allowing them to discover files quickly when needed, as well as begin to leverage the information they contain for regulatory and non-regulatory business objectives.

## Conclusion

---

### **BUSINESS & GOVERNANCE FOCUS: EMM Check List**

Denial is often IT's worst enemy. If you're unsure about your current email situation, perform a quick assessment of your current email infrastructure and ask yourself the following questions:

- ✓ How ready are you if the CxO comes knocking?
- ✓ How sure are you that your email applications meet corporate governance and regulatory requirements (e.g., retention periods, RTOs, etc.)?
- ✓ What business benefits, if any, do you derive from your email applications? Do you have an "information-centric" view of your business?
- ✓ Are your email management costs out of control?

We are entering a new era of information archiving where the needs of the business to access, share, and maintain an accurate historical record of business transactions and electronic records meets or exceeds IT's standing mandate to simply provide "another copy" of data in the event of data loss or disaster.

While we have only glimpsed the tip of the iceberg with regard to the impact that issues like regulatory compliance and corporate governance will have on the methods by which organizations manage information through its lifecycle, compliance is merely one of many drivers forcing IT and business leaders alike to reconsider the enormous scope of their archival requirements.

Likewise, we still find ourselves in what amounts to the early morning hours of the Information Age - we've really just begun to understand information as a discreet asset, or the power of information sharing and

collaborative development; none of which are able to be fully realized without a truly intelligent and active archive. Information, being a dynamic and fluid element, must be managed, protected, and ultimately preserved and made available for future use by technological solutions that are intelligent, adaptive, and scalable.