

**PROPER EMAIL
GOVERNANCE FOR THE
PROTECTION OF YOUR
BUSINESS AND BRAND:
THE BUSINESS CASE FOR
EMAIL ARCHIVAL ON
SECURE NETWORKED
STORAGE**

**A Frost & Sullivan White Paper Sponsored by
EMC
Analysts and Authors: Benoit Denis, Consultant
and Jarad Carleton, Senior Consultant**



TABLE OF CONTENTS

TABLE OF CONTENTS

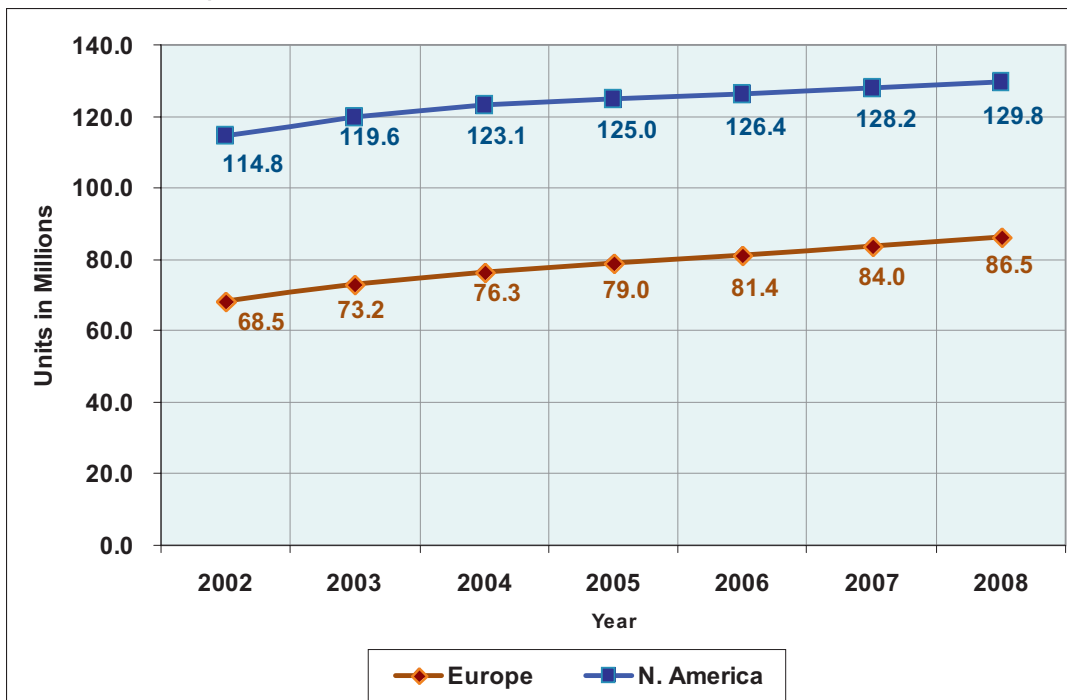
Introduction	3
Business Trends for Email Archiving in Europe	5
Business Trends for Email Archiving in the Americas	6
Email Archiving and Your Organization: Is Your Archiving System in Order?	7
Frost & Sullivan Viewpoint Regarding Email Archiving and Networked Storage	9
EMC Centera™ Content Addressed Storage (CAS) System and Email Archiving	10
Conclusion and Assessment	12

INTRODUCTION

The growing penetration of business email over the last ten years has placed email neck and neck with the telephone as the business communication medium of choice. In fact, depending on the business, email might be viewed as more useful and flexible than the telephone. In a world that increasingly relies on email to create and/or send the majority of business content today, it is critical that organizations meet the challenge of implementing policies and directives for email management.

An inability to create definitive policies and procedures for email management is most often the result of business needs that conflict with a user's legitimate requirement for instant access to all email, including old messages, for reference or repurposing. While users often require instant access to email regardless of its age, email administrators continually struggle to maintain high service levels while simultaneously enforcing retention and disposition policies that protect an organization. The fact of the matter is that an organization's ability to maintain and leverage large quantities of email is directly proportional to the robustness, as well as the ease of management and use of the email archive.

Business Computers with Email Access: Europe and North America (Canada, Mexico, & U.S.)



Note: All figures are rounded. Source: Frost & Sullivan

Therefore, it is important that when an organization is reviewing the effectiveness of a proposed email archiving solution that it carefully considers the following questions:

Does the solution provide the organization with:

- fast access?
- assured content authenticity?
- the ability to enforce retention and disposition policies on an item basis?
- ease of use and management?

These questions are viewed by many as critical towards the establishment of an archiving system that meets the needs of businesses today. The fact that so many organizations are asking these types of hard questions is exemplified in the responses companies gave to Cohasset Associates for the “Electronic Records Management Survey.” It was revealed in the survey that up to 59 percent of organizations continue to lack a formal email retention policy.¹

The lack of retention policies is compounded by the antiquated state of email archival and backup procedures employed by many organizations in Europe and the Americas. The Cohasset study showed that 93 percent² of organizations believe that electronic records will be important in future litigation, with many keeping their backup tapes for extended periods of time (usually years or decades). This is where organizations frequently err. They try to use email backup tapes as an email archive, a mistake that carries with it significant consequences in terms of business continuity and electronic discovery for a court case. This is due to the fact that tape as a media provides neither speed nor information authenticity. Therefore, trying to find a specific email on one of any number of incremental backup tapes is an onerous if not impossible task.

Beyond retrieval the use of tape as an archive places an organization at higher risk of losing data due to media degradation and improper “writes” to tape. Recovering from tape, especially when stored offsite, significantly lengthens response times to requests made by business users, compliance officers, internal audit, legal discovery teams working on time sensitive projects, and regulatory agencies. Examples abound of negative impacts on an organization’s productivity and budget when corrupted email stores and personal archives (.PST and NSF files, for example) have taken far too long to correct because the restore of emails was from backup tapes or a tape-based archive.

Finally, proper disposition of email is just as important as retention. Timely and permanent disposition of messages after a mandated archiving period is important to ensure that the organization complies with industry regulations and follows internal control procedures established through corporate governance initiatives. Finding and destroying archived email messages when they are scattered across various offsite tapes is often overlooked. In short, email archiving and backup is only effective if the company adheres to defined retention and disposition policies and leverages an intelligent archiving infrastructure.

Email archiving vs. email backup

Archived email is taken off of active production email servers and put onto a constantly available IP-based storage archive for purposes of easy retrieval and long-term retention. The policies are set by the email archiving software and can archive emails based on a number of factors, such as date of last access or size.

Email backups occur as part of a disaster recovery plan when incremental sets of email messages are stored for restoring the current email store.

In a world where business continuity, regulatory compliance, legal discovery, and risk mitigation are important, archiving and backup are two distinct terms.

1. Williams, Robert, F. Electronic Records Management Survey: A Call To Action. Chicago, IL, USA: Cohasset Associates, 2004: 36. 14 March 2005.

<<http://www.merresource.com/whitepapers/survey.htm>>

2. Ibid, p. 30.

Over the past four to five years there have been an increasing number of organizations that understand the difference between backing up email servers and archiving email. These organizations leverage storage technologies that provide fast access, ensure information authenticity, lower IT costs, and meet corporate governance and compliance requirements. By using this type of archiving solution, companies are able to decrease organizational risk by enforcing uniformly their retention and disposition policies. Organizations throughout the world that follow the best practices developed in the EU and the United States are expected to be in the best position to comply with new archiving regulations. As email use continues to grow annually in Europe and the Americas, the distinct and significant benefits of email archiving have become evident and commonplace.

BUSINESS TRENDS FOR EMAIL ARCHIVING IN EUROPE

The inherent weakness of tape storage solutions to enforce message retention and disposition policies across an organization and its inability to ensure data integrity over multiple years has begun to force a shift in the way that email is archived. Over the past few years, European businesses have slowly moved away from tape and optical media to traditional networked disk storage in an effort to improve access speed to information, email backups, and operational efficiency in areas such as reducing IT costs, and ensuring high levels of business continuity.

The European Union (EU) had, until recently, no unified law on email retention. Some members imposed no legal requirement while others had specific levels of requirements. The Data Retention Directive³ won approval from the European Parliament on Wednesday 14 December 2005 and is a new step towards regulating email management in Europe. The Directive has been encouraged by countries such as Ireland, Spain and the United Kingdom (UK), which are determined to fight organized terrorism by forcing companies, primarily in the telecommunications industry, to retain customer transactions such as telephone calls, website traffic, and email for a period ranging between 6 months and 2 years.

Not only do organizations have to keep records of transactions for a set amount of time, they must ensure that these records are unaltered during the retention period and must also ensure that the records are permanently disposed of after the retention periods are met. However mail servers and off the shelf disk-based storage cannot enforce retention and disposition policies, ensure data authenticity, or protect data from accidental and intentional deletion. These are key reasons organizations are turning to write once, ready many (WORM) disk-based storage.

For most organizations in the EU, email is the primary method of communication. Understandably therefore, email contains in excess of 80 percent of the business-critical content for an organization, such as attachments holding trade secrets and other types of confidential information. As a result, retaining these communication records and ensuring the authenticity of the email content is the only way to comply with data retention regulations now and in the future. It is expected that an increasing number of European

Compliance vs. Governance

Corporate governance consists of company policies that address a company's assets and employees. These policies are often associated with internal controls, operational efficiency, or both. Internal controls refers to the rules a company implements for information lifecycle management (data migration, retention, and disposition) whereas operational efficiency pertains to lowering operational costs, increasing worker productivity, and improving financial performance.

Corporate compliance occurs when a company implements policies in order to obey established laws and regulations in the nation or state where it conducts business.

Quite often, the only difference between the two is the organization requiring adherence - the Company (governance) or the Government (compliance).

3. "Information Dossier – Counter Terrorism." European Union, Justice and Home Affairs, Counter Terrorism Package. 28 June 2006.
<http://ec.europa.eu/justice_home/news/information_dossiers/counter_terrorism/index_en.htm>

governments will adopt stricter email and data retention rules over the next 5-10 years similar to what the Financial Services Authority has done in the UK which requires financial services firms to archive business email for 6 years. This in turn is expected to encourage stronger EU level directives pertaining to data retention laws.

Prior to the EU data retention directive, European organizations were focused on email archive infrastructure improvements out of a desire to address internal controls, corporate governance initiatives, and to protect brand equity. In fact, protecting brand equity by fostering an impression of openness to requests for information remains an overriding thought in the minds of European business executives and continues to be a top issue of concern for German businesses.

The simple fact is that the ability to properly and efficiently manage the lifecycle of email is viewed by many organizations in Europe as an important risk-mitigation step. The bottom line for many EU organizations is that proper email lifecycle management decreases outside liability potential and falls in line with modern corporate email governance procedures.

BUSINESS TRENDS FOR EMAIL ARCHIVING IN THE AMERICAS

Initially email archiving was put in place for compliance with government regulation. Over time however, it has evolved to be just as critical for internal operational efficiency and governance. This need is based on the growing concern for business continuity as well as strong process improvements and expense reduction. Key regulations in the U.S. market that require the retention of all formal and informal email, attachments, and instant message conversations include, but are not limited to:

- **Sarbanes-Oxley (SOX)** – Pertinent to all companies that are publicly traded in the United States regardless of where those organizations were incorporated. Titles 3-5 discuss maintaining an internal control structure, which has obvious email message implications.
- **Gramm-Leach-Bliley (GLB)** – Requires secure storage of personal financial information that frequently turns up in email and email attachments.
- **SEC Rule 17a-4** – Requires the retention of electronic or paper-based records by certain exchange members, brokers, and dealers.
- **SEC Rules 31a-1 and 31a-2** – Addresses electronic correspondence retention for mutual fund companies.
- **SEC 204-2** – Applies to electronic correspondence for investment advisors.
- **NASD 2210, NASD 3010, and NYSE 342** – Outline codes of conduct around paper and electronic correspondence.

- **HIPAA** – Requires the protection of healthcare data for individuals in paper and electronic form. In the era of patients emailing healthcare questions to their doctors, HIPAA clearly has implications on email security, retention, and eventual disposition.
- **TREAD** – Requires all automotive manufacturers and automotive importers of vehicles sold in the U.S. to retain a wide variety of automotive data, some of which is created and forwarded via email.
- **California Personal Information and Privacy Act (SB-1386)** – Requires all organizations in the public and private sectors to disclose any breach of data security to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Organizations are struggling with these and other government mandated requirements to retain and protect enormous amounts of email, while also providing fast access, ensuring information authenticity, and enforcing uniformly the retention and disposition policies of an organization. In order to comply with so many different regulations, the public and private sectors have begun to favor a networked disk-based storage infrastructure that is much easier to manage and provides rapid response times to government agencies and legal team information requests that would otherwise be impossible to achieve with a tape or optical archive solution.

Rapid response to information requests helps businesses access information quickly, but only by assuring content authenticity can an organization avoid fines and minimize negative media attention. Assuring email authenticity and integrity is not a feature offered by traditional networked storage solutions. And as in Europe, these requirements are a key reason that organizations based in the Americas are more frequently seeking to leverage online disk-based WORM storage solutions for email archiving.

EMAIL ARCHIVING AND YOUR ORGANIZATION: IS YOUR ARCHIVING SYSTEM IN ORDER?

Despite all of the attention given to email archiving in the Americas and E.U., newspaper headlines continue to prove that many organizations in the public and private sectors continue to use email archiving policies that have not kept pace with changing legal standards. Email archiving policies should be reviewed and updated if any of the following points apply in your organization:

- **Email Storage Limits** – Putting limits on the size of an email inbox does help email administrators to manage the email system, but it also forces users to create local email archives that become unstable and susceptible to data corruption as the local archive grows.

- **Local Email Archives** – When business users create local, private email archives on laptops and desktops, they place the organization at risk of outside liability. This is due to the fact that local archives are not centrally managed and emails that should have been destroyed after a mandated retention period expires are not. This can subject the organization to embarrassing situations, fines and more.
- **Email Server Backup Windows** – With the increasing volumes of email exchanged in today’s global business environment backup windows become harder to meet. Failing to meet a backup window will not only effect Service Level Agreements (SLAs) and recovery times but can also put an organization at risk of not being able to produce complete email records during eDiscovery requests.
- **Email Archives on Tape** – The risk an organization takes with tape storage as its email archive is multi-pronged in that data on tapes is hard to manage, can be corrupted as the media degrades, and requires an expensive and onerous process in order to respond quickly to eDiscovery requests. In addition, when tapes are misplaced, information provided during eDiscovery requests is incomplete and subjects an organization to possible fines and remedial action.

Because many of the points above apply to organizations operate in the Americas. and the E.U., there is an increasing realization that new ways must be found to preserve emails for mandated retention periods as well as to protect operational efficiency and business continuity.

In fact, operational efficiency as it pertains to email archives has far more importance than ensuring high productivity levels and lower storage management costs. Regulations such as SOX and BASEL II (the International Convergence of Capital Measurement and Capital Standards) effectively pierce the corporate veil and hold executives civilly and criminally responsible for noncompliance. In order to protect the organization and its employees from a damaged reputation, fines, or loss of individual freedom, forward thinking organizations are taking a proactive approach to implementing disk-based WORM email archives that will ensure data integrity and establish data authenticity.

Whereas BASEL II is an international accord followed by financial services firms in the major centers of banking around the world, SOX is a regulation that only applies to the U.S. market. That means that all companies, regardless of origin, that have stocks listed and traded in the United States must comply with SOX. Although the EU doesn’t regulate publicly traded companies with a law similar to SOX, most European businesses consider new regulations at national levels such as those based on the EU Data Retention Directive as inevitable and are starting to prepare.

FROST & SULLIVAN VIEWPOINT REGARDING EMAIL ARCHIVING AND NETWORKED STORAGE

In organizations where storage technologies such as tape, optical, and traditional disk-based storage are used for email archiving, legal discovery and regulatory compliance response times are frequently drawn out. When an email archiving application is not used in conjunction with disk-based WORM storage, it is possible for the authenticity of information to be questioned. In this type of situation, an organization's claim of uniformly applying their retention and disposition policies can also be called into doubt. These were the types of reasons given by 62 percent of organizations polled in the Electronic Records Management Survey when they responded that they were either "not at all confident" or only "slightly confident" that they could demonstrate electronic records were accurate, reliable, and trustworthy.⁴

Regardless of the reasons behind delayed responses to eDiscovery requests, failure to respond quickly can create serious problems up to and including:

- Contempt of court charges
- Jail time for executives
- Fines and remedial actions
- Negative press and brand damage

Whether in Europe or the Americas, an email archiving application that is tightly integrated with disk-based WORM storage is the best way to ensure nonrepudiable data authenticity as well as enforce uniformly an organization's retention and disposition policies.

Leveraging robust email archiving software either as a standalone application or as part of an enterprise content management application, with a purpose-built archiving storage platform is a key component of any organization's information lifecycle management (ILM) strategy for email. Through the establishment of archiving policies within the email archiving application, emails of a certain size or age can be automatically migrated from the email server to the archive. This in turn helps email administrators ensure that the backup of email stores are completed within established windows, in accordance with service level agreements (SLAs), and without the need to purchase new email servers.

In addition, by enabling automatic movement of emails containing large attachments and older emails from the email server to an online archive platform, businesses regain space on email servers while still allowing end-users to access all of their archived messages. Leveraging disk-based WORM storage as an email archive provides fast 24/7 access to archived messages, creates a mail box with limitless storage, and ensures data authenticity and cost effectiveness. This is critical not only for regulatory compliance, but also for business continuity and corporate governance initiatives that focus on both improving productivity and lowering storage management costs.

4. Ibid, p. 33.

EMC CENTERA™ CONTENT ADDRESSED STORAGE (CAS) SYSTEM AND EMAIL ARCHIVING

The need to have unlimited access to all email continues to increase each year and negative consequences and costs can arise when users are subjected to limitations or incomplete email archive solutions. Forcing users to delete messages due to archive functionality or cost constraints, creates an unintentional incentive for users to create unmanaged local email archives that, as mentioned before, are susceptible to data loss, misuse, and increase outside liability risk when eDiscovery requests arise. This approach is no longer acceptable nor is it necessary with EMC Centera™ and its Content Addressed Storage (CAS) technology.

EMC Centera™ CAS technology stores and retrieves email and other information based on a Content Address (CA), not the information's physical or logical placement within the storage array. This dramatically reduces system and storage management.

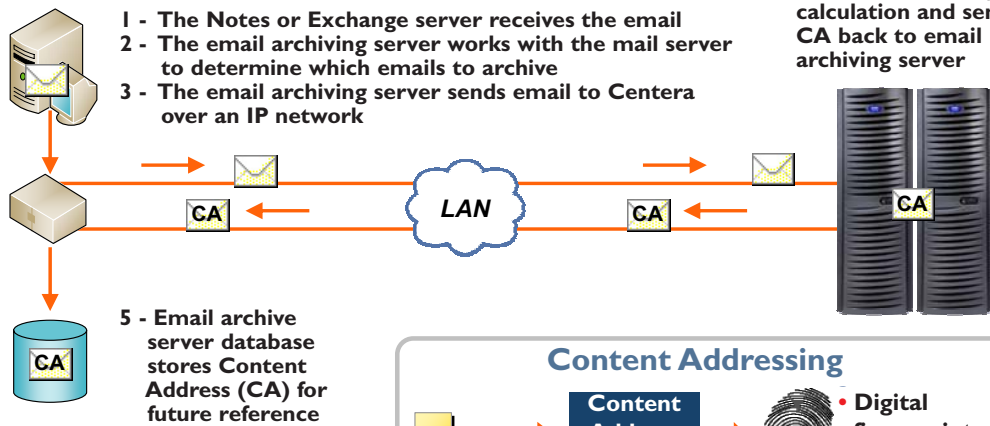
An EMC Centera™ CA is the identifier to the content (in this case email) as well as a digital fingerprint for the stored information. It ensures data security and authenticity both of which are vitally important to businesses across industries and geopolitical boundaries that need to maintain internal controls, business continuity, corporate governance and compliance, as well as respond to eDiscovery requests.

As disk storage, EMC Centera provides online access to archived email. As a digital fingerprint of the content an EMC Centera™ CA improves daily email archiving operations by eliminating duplicate copies of information from being stored. If two people try to store the same content, EMC Centera will compute the same CA twice, stores the content once, and gives both users pointers to the common object. This applies whether the two people or one thousand people store the same file, in each situation only one copy of a file is kept. In the event that content is altered, EMC Centera™ computes a different CA (because the content is different) and stores the altered content. This ensures that data is never overwritten when users create different versions and guarantees that content cannot be repudiated during eDiscovery requests.

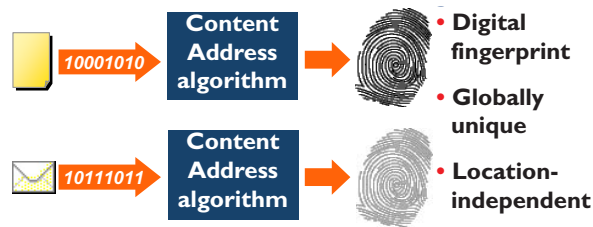
When email is archived to EMC Centera™, both the stored email and metadata describing the email are kept and both are given a CA. The XML based metadata file (also referred to as a C-Clip Descriptor File or CDF) is specific to each individual's use of the common object or email. It is the metadata file that allows multiple people to annotate content as business needs dictate and enables different retention and disposition policies on a piece of unique content while only storing one copy. The CDF is then protected in the same way as the object itself and is the mechanism used by an application to retrieve an information object. Retrieval of content within EMC Centera™ is based entirely on Content Addresses rather than a centralized directory, pathnames, or URLs.

How Centera Works: Email Archiving

4 - Centera performs Content Address (CA) calculation and sends CA back to email archiving server



Content Addressing



For business continuity purposes, EMC Centera™ stores, secures and protects content locally using content mirroring or content parity protection and allows content to be replicated to another EMC Centera™ system. In the event that a disk drive fails, EMC Centera™ detects the fault, and uses the mirror or parity to generate an additional copy of any emails on the failing drive(s). As this process takes place, the affected drive(s) is isolated from the rest of the system and can be hot swapped without disruption, as applications don't have knowledge of the physical placement of content within EMC Centera™.

One thing is clear for executives across all industries and organizations, businesses operating in the EU and the Americas have an increasing need to enforce uniformly their retention and disposition policies. Both EMC Centera™ Governance Edition and Compliance Edition Plus enforce an application's retention policies within the storage, no matter how complex the policies. EMC Centera's functionality is especially beneficial to the 46 percent of organizations that do not have a formal system in place to lengthen retention periods.⁵

In the case of eDiscovery, a legal team could spend substantial amounts of time searching tape and optical storage media to find and classify emails related to a case. EMC Centera's online access coupled with CenteraSeek™ provides users with an enhanced cross-application search engine that utilizes the EMC Centera metadata for very fast search and retrieval of needed content. This in, conjunction with Governance Edition or Compliance Edition Plus, enables legal teams to more easily place litigation holds on email related to a case and ensure that content will not expire during litigation. Lastly, CenteraSeek™ is also

5. Ibid, p. 21.

used by internal audit, human resources, research and development, and other departments needing to maintain internal controls.

Although email retention is important, the disposition of email immediately following the end of a retention period is equally significant. EMC Centera™ offers organizations the ability to achieve permanent disposition of email in accordance with the U.S. Department of Defense 5015.2 directive for data deletion.

CONCLUSION AND ASSESSMENT

EMC Centera's™ ability to provide fast access, non-repudiable information authenticity, enforce retention and disposition policies and reduce system management costs helps organizations address complex email archiving needs and cost constraints.. It should also be noted that while this paper discusses EMC Centera™ in terms of email archiving, it can archive all content types from any application or platform.

In short, EMC Centera™ offers companies a flexible and field tested archive storage platform. Whether solely for email or as a multi-application repository EMC Centera™ offers organizations a lower TCO than tape and optical storage and increased operational efficiency. As the catalyst to consolidate an organization's storage infrastructure, EMC Centera™ is able to restrain, and in some instances slow to a crawl, the annual growth of an organization's storage expenditures. As a result, it is possible for many organizations to achieve a positive ROI on their EMC Centera™ implementation within the first 12 months, making it a storage solution that should be seriously evaluated as part of a cost reduction and corporate governance program.

With the continued rapid growth of email in both Europe and the Americas, organizations cannot take a wait-and-see approach to email archiving when there is so much at stake legally and financially. The decision to implement a critical infrastructure improvement solution such as EMC Centera™ for email archives can no longer be sidelined.

CONTACT US

Bangalore

Bangkok

Beijing

Buenos Aires

Cape Town

Chennai

Delhi

Dubai

Frankfurt

Kuala Lumpur

London

Mexico City

Mumbai

New York

Oxford

Palo Alto

Paris

San Antonio

Sao Paulo

Seoul

Shanghai

Singapore

Sydney

Tokyo

Toronto

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your organization, and thereafter it may not be recopied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write:
Frost & Sullivan
2400 Geng Rd., Suite 201