

## EMAIL ARCHIVING

Planning, policies and product selection

---

# CHAPTER 3 Choosing email-archiving product features for compliance and risk reduction

- 03 Email-archiving system architectures
- 05 Compliance features
- 08 Litigation support features

*Companies need to make compliance and litigation support a top priority in their email-archiving systems.*



# CHAPTER 3 | Choosing email-archiving product features for compliance and risk reduction

by Marion Weiler  
and Kathryn Hilton

THE MOST IMPORTANT PART of implementing an email-archiving system is defining email-retention goals and policies. Precise goals and policies can help IT departments clarify which features in an email-archiving system meet corporate needs, particularly in the area of risk reduction for compliance and litigation support.

Although policies can motivate companies to consider an email-archiving system, business decisions generally drive the implementation. Reducing the risk of litigation through regulatory compliance is one of the main reasons that organizations are exploring email-archiving systems.

Another reason is improved productivity. End users and IT departments alike can benefit from features such as mailbox management that are available in email-archiving systems. Email-archiving product features that relate to end-user productivity will be explained in more detail in the next chapter.

Before we examine the compliance and litigation support features you need to consider when evaluating an email-archiving product, let's review the three basic email-archiving system architectures available on the market.

## Email-archiving system architectures

*Architectures for email-archiving systems fall into three categories: hosted solutions, in-house solutions, and hybrid solutions.*

**HOSTED SOLUTIONS** require minimal on-site hardware and software. In a hosted solution, company email is copied and sent for storage at the vendor's location. Interfaces are available so that employees who have been designated by the company can search and retrieve archived email. This type of solution provides no integration with the end-user desktop and is typically used where compliance and litigation discovery are the only goals.

**IN-HOUSE SOLUTIONS** store all hardware and software on site and are usually managed by individual companies. This type of solution typically addresses end-user productivity, storage management and compliance goals. It also allows a high degree of control and integration with the end-user's desktop.

**HYBRID SOLUTIONS** are a cross between hosted and in-house solutions. Some software and hardware components are on site, but the vendor maintains and manages the overall system. This type of solution is often used for its end-user features but eliminates the need to own and operate the archiving system. Companies can use hybrid solutions to avoid adding internal IT staff, to respond quickly to scalability issues, or to stay current with the latest versions of the software and hardware.

JUST AS COMPANIES vary in their goals and requirements, each email-archiving vendor differs in its product offerings and feature sets. If your company's goals focus on mailbox management, then consider in-house or hybrid solutions. To address compliance or litigation support goals only, you may want to consider hosted solutions.

For integration with an existing IT architecture, develop a

Understanding your system's architectural integration needs will help you define your email-archiving product feature requirements.

detailed list of features that define the company's existing IT architecture and the important integration points. Particularly when it comes to responding to regulatory agencies or document discovery requests, it is important that your archive system is fully functional and that service levels can be met. Architectural elements to consider include:

- **The operating system** (Windows, Linux)
- **The email server** (Microsoft Exchange, Lotus Domino, Unix Sendmail)
- **The desktop email client** (Microsoft Outlook, Lotus Notes, Web mail clients)
- **Network protocols** (TCP/IP)
- **Directories** (AD, LDAP)
- **Storage infrastructure** (NAS, SAN)
- **The application-monitoring system and alerts**

- **Strategic relationships with particular vendors**, especially storage vendors that provide optimal pricing and overall service integration

Understanding the architectural integration helps define the required features for each area. Most organizations use a phased approach, which solves high-risk priorities first before looking at productivity and cost savings. Finally, they develop requirements as a starting point for discussions with internal stakeholders and external vendors as well as analysts.

Consider what the requirements are for related IT systems and decide what features they may need in an email-archiving system. Some email-archiving systems have features that enable archiving other objects, such as files and instant messages. These objects may be related to corporate reten-

tion policy and plans.

One feature to consider is hosted spam filtering, which quarantines items before they hit the email server so that less spam is archived. Compare this feature to spam-filtering tools that pass all items to the user's mailbox.

A unified messaging plan is another feature. These plans incorporate voicemail messages into email servers. If an email-archiving system includes voicemail integration with the email, then the organization may require specialized features for voicemail messages—for example, the ability to apply different retention schedules to voicemail or to access specialized search engines that can handle voice files in response to regulatory or litigation discovery needs.

Encryption is another element to consider. An email-archiving system that uses encryption

can detect encrypted items and archive them in an unencrypted format, not archive them at all, or just archive the items encrypted and un-indexed. In general, however, it is not a good idea to archive encrypted items unless they can be decrypted on demand. Courts may consider an archived item that cannot be decrypted in response to a discovery request as spoliation, or destruction of evidence.



Look for the ability to conduct unified searches across the email archive using high-performance search engines and the ability to apply and maintain granular retention schedules, by group, individual or job title.

## Compliance features

*Compliance generally refers to obeying government regulations that dictate what data companies need to keep. For some organizations, such as broker-dealer shops, compliance means capturing a copy of every email sent and received by brokers and the employees who closely support them.*

TO UNDERSTAND REGULATORY compliance features, companies must know the regulations under which they operate. Many factors determine the types of regulations that govern an industry, such as healthcare, banking or transportation. Geography can also play a role—businesses that are based in the United States, for example, follow somewhat different regulations than those that are based overseas. Some countries may even have in—country data-retention

requirements or data-privacy regulations that other countries do not have.

The type of workforce can be a factor in compliance, where primarily exempt employees may have different regulations to follow than those who work in a highly unionized shop, for example. Companies that are publicly traded or privately held have different compliance regulations.

Some regulations that define retention standards can specify what data to save, how to save

it and whose communication to keep, as in the case of brokers. Other regulatory issues spell out how long the minimum or maximum data-retention periods are. Access and timely retrieval for producing records on demand as well as security to prevent unauthorized access may also be specified in regulations.

Searching and retrieving archived email quickly in response to regulatory requests and providing external parties, such as your external law firm, secure direct access to the archiving system to perform their own discovery operations are more capabilities that IT managers might consider when looking for an email-archiving system.

To assist with these requirements, look for the ability to conduct unified searches across the email archive using high-performance

## IT managers should start with the corporate compliance officer or the compliance group to determine which regulatory features relate to their email-archiving systems.

search engines and the ability to apply and maintain granular retention schedules, by group, individual or job title.

How email is stored can be regulated as well. The storage of archived email items on non-erasable, non-rewritable media or the storage of items in their original format with the original metadata are two areas that may be governed by regulations, so IT managers should look for features that can accommodate those requirements.

Features such as monitoring or intercepting outbound email message traffic and preventing

it from being captured in the archive are other valuable features. IT managers may also need the ability to protect personally identifiable information and dispose of it when it is no longer needed.

Each regulation may differ in exactly what it specifies, so each company must know which regulations apply. IT managers should start with the corporate compliance officer or the compliance group to determine which regulatory features relate to their email-archiving systems.

# All content and no discovery?



**Lost in a maze of unmanageable content? Find your way out with Enterprise Vault. It's a flexible archiving framework that enables the discovery of content within email, file system and collaborative environments. Reduce costs. Simplify management. Put your discovery fears behind you at [www.symantec.com/compliance](http://www.symantec.com/compliance) **BE FEARLESS.****

Copyright ©2005 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.



## Litigation support features

*While compliance features keep data for specified periods of time and produce data on demand for regulatory authorities, litigation support finds and produces whatever data the company has that relates to the legal issue at hand. Unlike compliance requirements, litigation support includes broad document discoveries that do not specify beforehand what data may be relevant. The feature requirements for compliance and litigation-risk reduction, however, do overlap.*

DON'T LOOK AT the email-archiving system as a full litigation case-management tool. An email-archiving system acts as a feeder system to the overall case-management system—but not a replacement for it.

### Features that support litigation include:

#### LITIGATION DESTRUCTION-HOLD FEATURES

- Applying an indefinite destruction hold to the archive or portions of the archive.
- Applying targeted destruction holds, based on flexible criteria that result from a search, to narrowly target the hold to items specific to the response.
- Allowing multiple destruction holds against one item.

- Releasing an individual destruction hold against one item, while leaving any others in place.
- Applying a friendly name to destruction holds, such as a case name or number.
- Providing a reporting function, or dashboard, for the destruction-hold function.

#### SEARCH AND RETRIEVAL FEATURES

- A robust search engine that allows searches by a number of criteria and methodologies. The search engine should meet the requirements of all involved in discovery efforts.
- Retrieval options for writing the results to the location and media of choice. For example, a specific file location on any network-accessible drive, CD or DVD.



- Search and retrieval documentation that is adequate to fulfill any chain-of-custody requirements from regulators, courts or opposing parties.
- Search and retrieval performance that meets the timeliness requirements for document production. Examples include response to regulatory requirements or the Federal Rules of Civil Procedure.
- Search-term lists that can be imported without having to manually retype them.
- Full-text indexing of all items as they are archived.
- Integration with the case-management tool of choice.
- Encryption capabilities.

#### AUDIT TRAIL FEATURES

- Developing audit trails for all accesses, search-and-retrieval actions and disposition activity.
- Documenting the chain of custody.
- Hiding audit logs and destruction holds from end users who are subject to investigation.
- Printing a summary of the retention schedule for the archive. The summary may include all the retention rules in force, categorized by criteria such as group and job level. It may also include a change history of those rules.

- Storing audit logs, including the retention schedule, as items in the email archive.

#### SECURITY AND ACCESS CONTROL FEATURES

- Inheriting the access controls that archived items had in the email system.
- Applying special processing to items marked with security classifications, such as confidential or attorney-client privileged communication.
- Reducing risk means making sure that all email is diverted to known, manageable locations. Keep the complete archive in one spot. Ensure the company has reasonable assurance that all email messages are deleted according to policy.

The bottom line is that companies need to think carefully about the email-archiving features they choose, using a top-down approach.



Every company has its own unique set of required features based on its goals and policies. Systems will vary based on the goals of each enterprise.

Start with company goals and policies, and mold feature requirements around them. Eliminate personal email archives. Run periodic sweeps of file servers and C drives to find personal archives, and publish policies against their use.

Provide end-users with a centralized email archive, and make sure to resolve conflicting feature priorities. Most of all, engage every party that has a stake in the outcome of your email-archiving system to share in its success.

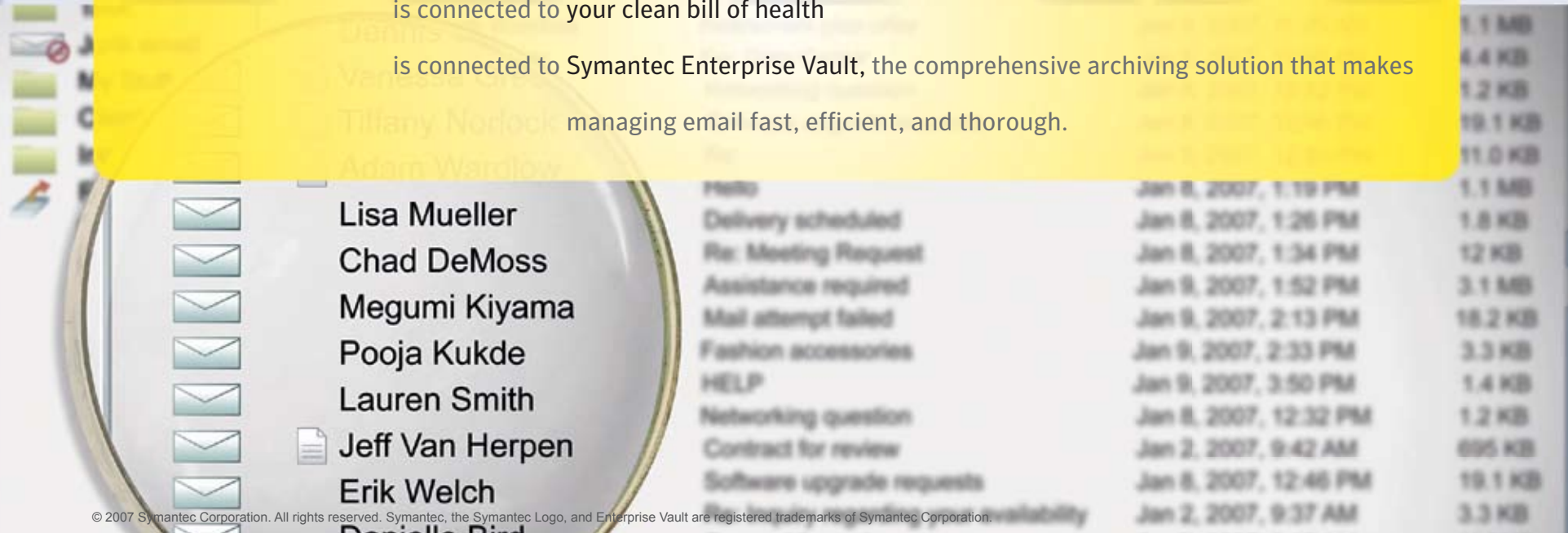
Precise goals and policies can help IT departments clarify which features in an email-archiving system meet corporate needs, particularly in the area of risk reduction for compliance and litigation support.

Features are not necessarily requirements and vice-versa. Before implementing any email-archiving system, IT managers should follow a process to help them correctly identify the features they need. That process can be broken down into the following steps:

- 1 Define project goals and company policies.
- 2 Use those goals and policies to develop requirements and features.
- 3 Understand that every company has its own unique set of required features based on its goals and policies. Systems will vary based on the goals of each enterprise.
- 4 Clarify project goals and priorities.
- 5 Know which features address conflicting or competing priorities.
- 6 Think through the requirements and related features in detail. Selecting general feature requirements often generates a list of more granular feature requirements and options.
- 7 Engage all groups with a stake in the email-archiving system for help in deciding on required features. Usually these groups include the various business units, the legal and compliance departments, and the IT department.



The legal investigation is connected to the discovery request  
 is connected to combing through terabytes of archived email  
 is connected to your clean bill of health  
 is connected to Symantec Enterprise Vault, the comprehensive archiving solution that makes  
 managing email fast, efficient, and thorough.



© 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Enterprise Vault are registered trademarks of Symantec Corporation.

**Take control of your most important digital assets.** Up to 75% of your company’s intellectual property is in email or instant messaging. Today, a typical eDiscovery request can cost IT departments countless hours and dollars to recover the specific range of messages on time. Symantec Enterprise Vault™ facilitates the legal and business best practices of storing, managing, and discovering email and other electronic files. So you’re free to focus on the big picture. [Learn more at symantec.com/enterprisevault](http://symantec.com/enterprisevault)

## About the authors

MARION WEILER *has worked in technology for more than 23 years, specializing in a number of areas including email archival, email systems design and management, and IT architecture. Weiler received a bachelor of arts degree in biology from the University of California, San Diego, and a master's degree in business administration from the University of Michigan, Ann Arbor. He is currently a senior analyst for policy at Contoural Inc., a technology consulting firm based in Mountain View, Calif., that focuses on litigation readiness, compliance, information and records management, and data storage strategy.*

KATHRYN HILTON *has worked in technology for more than 20 years as an industry analyst for Gartner Group and for several large storage companies. Hilton received a bachelor of arts degree in business economics from the University of California, Santa Barbara, and a master's degree in business administration from the University of Colorado Leeds School of Business. She is currently a senior analyst for policy at Contoural Inc., a technology consulting firm based in Mountain View, Calif., that focuses on litigation readiness, compliance, information and records management, and data*

## Additional resources from Symantec

### Learn more about Symantec Enterprise Vault

Symantec Enterprise Vault 7.0 provides a software-based intelligent archiving platform that stores, manages and enables discovery of corporate data from email systems, file server environments, instant messaging platforms and content management and collaboration systems.

**For a variety of white papers, case studies, testimonials and more,**  
[CLICK HERE.](#)