Symantec Enterprise Vault™ Data Classification Services

Providing context and relevance for managing and retaining email

Data Sheet: Archiving

Overview

Email archiving helps to facilitate the long-term retention, management and discovery of information to optimize IT efficiencies and lower business risk. But as messaging volume grows, organizations are becoming increasingly interested in controlling storage and operation costs by utilizing message classification.

By automatically classifying email (for example, as business, personal or garbage), organizations can zero in and decide whether or not to store a message. They can then set granular retention policies across different categories of information and determine the optimal storage media to utilize—helping to significantly lower operations costs as they keep the size of the archive in check. Additionally, accurate classification of messages provides context and relevance, enabling easier retrieval and processing.

Key benefits

- Automatically classify and archive Microsoft® Exchange email based on metadata and content, including attachments.
- Lower storage costs and resources.
- Avoid archiving garbage or irrelevant content (for example, newsletters or bounce messages).
- Provide context and insight into what is archived.
- Enable granular retention, delete with confidence.
- Search and review faster and more efficiently.
- Share classification policies with Symantec™ Data Loss Prevention.

Symantec Enterprise Vault™ Data Classification Services

Enterprise Vault Data Classification Services extends the existing capabilities of Enterprise Vault to include intelligent, content-based categorization and tagging of Exchange email using content or context.

Data Classification Services enables content-aware archiving by:

- Determining whether or not email needs to be archived, or even discarded.
- Assigning appropriate tags to email. One tag may correspond to a retention category, which determines how long the email is retained in the archive. Another may relate to high risk data (for example, credit card numbers, intellectual property or inappropriate language), helping speed reactive eDiscovery or proactive supervisory review.
- Enabling greater efficiency using the Symantec Enterprise Vault™ Discovery Accelerator and Compliance Accelerator tools. These tools leverage the tag categories to enable managers to zero in on items of interest when searching for and reviewing archived email, or including or excluding content for review.

How it works

As an Exchange message is archived, the Enterprise Vault server automatically forwards it to a Data Classification server, which analyzes metadata, content and attachments against policies (see Figure 1). Policies determine how the message is treated – whether or not it will be retained, and whether or not one or more unique tags will be attached to the message. If policies deem the message must be retained, it is allowed to continue, potentially with classification tags, to the Enterprise Vault archive. Otherwise, the message is not archived, and you can optionally configure that it be automatically deleted.
Because Data Classification Services is built on Symantec™ Data Loss Prevention technology, you will be able to share policies between solutions. That means the policies you create with Data Loss Prevention may be used with Symantec Enterprise Vault Data Classification, and vice versa, although the response you configure will likely be different for each solution. Still, this ability to share policies – and Data Classification Services ships with 70 pre-configured policies out of the box – between solutions provides you with a consistent, unified approach for protecting, managing and retaining information.

![Figure 1. Symantec Enterprise Vault™ Data Classification Services Architecture](image)

Retain only what is meaningful to your organization

Although the ability to configure retention folders within a mailbox to allow the end user to classify and retain email exists, the process is still manual, and you’re actually at the mercy of your end user as to whether a particular message was classified correctly. Why not automate the process to instill consistency and remove any doubt? Enterprise Vault Data Classification Services does just that by enabling you to automatically enforce unique email retention – based on content, source and people involved – if the message is deemed meaningful per policy. If not, leverage policies to ensure junk mail, garbage and other non-business records are not archived and are optionally deleted. This helps control the size of your archive, while giving you confidence in knowing exactly what information is being retained.

Lowering costs of eDiscovery and enabling regulatory compliance

Enterprise Vault Data Classification Services helps staff responsible for legal and regulatory compliance to rapidly identify and access the highest priority communication they need in order to retrieve, review, audit and produce documents. This is accomplished through tagging, and during the review process, authorized users can use Symantec Enterprise Vault™ Discovery Accelerator to filter results. Customizable tags can be used to exclude messages, such as privileged communications, when responding to a subpoena or preparing for litigation. Tagging also integrates with Symantec Enterprise Vault™ Compliance Accelerator, helping set priority to items that should be proactively reviewed (for example, inappropriate communications, policy violations, Human Resources issues, etc.)

In the end, Data Classification Services gives organizations the ability to control what is in the archive and locate the email content they need quickly, helping to lower the costs associated with reactive eDiscovery and proactive supervisory review.