Overview
Today’s regulatory climate has created email communication issues for broker-dealers and financial institutions of all sizes. Companies rely heavily on email in order to compete. But as the volume of email traffic grows, so does the challenge of meeting various SEC, FINRA, and NYSE compliance requirements.

Deliver simplified, cost-effective email retention and supervisory compliance
Symantec Enterprise Vault Compliance Accelerator is a highly configurable add-on solution to Enterprise Vault for Microsoft® Exchange. Compliance Accelerator allows organizations to perform cost-effective supervisory review of broker-dealer email to help ensure compliance with regulatory bodies. Providing the framework to select and sample target email, manage its review by appropriate reviewers, and record the process for audit purposes, Compliance Accelerator helps to decrease the cost and effort of email supervision, review, and compliance demonstration.

Key benefits
- Address SEC 17a-4 and FINRA 3010 and 3110 email retention and compliance requirements
- Significantly facilitate and help lower the cost of email supervisory process
- Reduce the administration load on reviewers and control end-to-end email supervision
- Quickly find and present relevant email for proactive email retention and response
- Demonstrate commitment to compliance and best-practice governance

How it works
Superior email content archiving
Working seamlessly with Microsoft Exchange and Lotus® Domino® environments, Symantec Enterprise Vault will archive and index messages and store them in their original form (email and attachments) centrally—with no impact on or intervention by users.

Enhanced email supervision, sampling, and review
Compliance Accelerator seamlessly extends Enterprise Vault functionality by targeting Enterprise Vault archives to supply proactive monitoring of email communication between individuals and groups—implemented without
huge administration or manual overhead. Compliance Accelerator allows structured review processes to be put in place to search, sample, and review journal archived email according to compliance policies. The entire process is tracked, and extensive reporting demonstrates adherence to corporate and regulatory compliance policies (i.e., the SEC, FINRA, and NYSE).

2) **Apply email sampling rules**

Customize to the legal department’s or the compliance manager’s needs.

- Sample all or per individual
- Percentage sample
- Minimum sample size applied
- Example—“Take a 5% sample of the mail between my group and group X from September 1, 2006 to December 31, 2006, with a minimum sample of 2 messages per person in my group.”
- Run search

3) **Review search results**

Through a Web interface, reviewers are presented with email to review. The status of each email is tracked and where further action is required, it can be flagged against the original email.

- All items start as Unreviewed and end as Reviewed or Questioned
- Reviewer can set Pending status while investigating
- Reviewer can annotate reviewed messages
- Reviewer can escalate messages where appropriate to senior Compliance supervisor
- Reviewer can launch Microsoft® Outlook® viewer to forward message
- Reviewer can close review sample when all reviewed
- Everything recorded and reported
4) Log

Keep an audit trail of the whole process. Should disputes arise, it is easy and straightforward to investigate what happened if the administrator can demonstrate that the audit took place.

- System configuration
- System users
- Group configuration
- User activity (searching, reviewing)
- Audit
- Audit trail of messages in review process

Compliance Accelerator product functionality

- **Fully managed and audited**—Compliance supervision/review process
- **Easy to use**—User model is a set of audited groups (e.g., dealer desks, branches), each with associated owner/reviewer doing regular reviewing
- **Highly flexible**—Potential target is all email, internal and/or external
- **Effective sampling**—Selective searching and sampling to produce items for review
- **Custom search**—Manual or automatic searching/sampling
- **Rapid deployment**—Tightly integrated with Microsoft Exchange and Lotus Domino, easy to install, transparent to users
- **Extension of Symantec Enterprise Vault**—Optimized storage, simplified management, and instant discovery

Prioritize review content by category

Applying context to archived content optimizes the compliance review process. Symantec Enterprise Vault Automatic Classification Engine (ACE) software extends the existing capabilities of Enterprise Vault to include intelligent, content-based categorization and tagging of email. Specifically, automated classification enables Enterprise Vault to apply rules to email and categorize messages according to content or context. This optional component can be leveraged in Compliance Accelerator to facilitate more effective review, because messages can be flagged for review by category. This helps target content to be reviewed and ensures that review staff examine high-priority content vs. irrelevant messages (e.g., junk and bounce messages)

**Intuitive, event-driven workflow and guided review**

- Organize and rapidly review search results using frequently occurring keywords, metadata and policy matches to organize the result set and marking process using guided review.
- Allow hierarchical initial review and case management by authorized reviewers.
- Review and mark individual items or result sets using customizable marks.
- Escalate individual items or result sets for further review by designated supervisors.

Symantec Enterprise Vault

Enterprise Vault, the industry leader in email and content archiving, enables companies to store, manage, and discover unstructured information across the
enterprise. Using a market proven architecture, Enterprise Vault provides an open, intelligent and manageable approach to improve management, reduce costs and control information risk. With unstructured information consuming a large percentage of corporate storage, Enterprise Vault archives information from messaging, file servers and collaborative systems using powerful storage optimization, classification and retention technologies. Enterprise Vault will automatically capture, categorize, index and enforce retention policies and secure unstructured information while reducing storage costs and simplifying management.

**Product requirements**

- Symantec Enterprise Vault 2007 (7.5) SP4 or later with basic configurable options for capturing targeted content (e.g., Microsoft Exchange or Lotus Domino Journaling)
- Dedicated Microsoft Windows Server® 2003 SP2 or Windows 2008
- 2 GHz Intel® Xeon™ or better dual processor
- 2–4 GB RAM
- Microsoft .NET Framework v3.0 SP1

Enterprise Vault allows customers to leverage existing storage platforms or implement more cost-effective storage specifically designed for archiving and long-term data retention. Storage options include:

- Direct attached storage (DAS)
- Storage area network (SAN), network attached storage
- WORM devices and content addressable storage (CAS)
- DVD/Optical/Tape (using Veritas NetBackup™)

For a complete list of requirements and supported hardware and software, please visit www.symantec.com.

**More information**

**Visit our Web site**

http://enterprise.symantec.com

**To speak with a Product Specialist in the U.S.**

Call toll-free 1 (800) 745 6054

**To speak with a Product Specialist outside the U.S.**

For specific country offices and contact numbers, please visit our Web site.

**About Symantec**

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

**Symantec World Headquarters**

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.