

Mimosa NearPoint Content Monitoring Option

Powerful Monitoring for Internal Governance, Protecting Information Assets, and Meeting Regulatory Requirements

Your employees represent your company. Like most organizations, your company likely reaffirms and emphasizes its commitment to maintain a workplace environment that's free from sexual harassment and other criminal activity. This activity can impact legal costs, employee productivity, shareholder equity, and cause damage to your corporate brand. Developing usage and code-of-conduct policies along with monitoring for compliance will insure an environment free from unwanted content coming in and the loss of sensitive company information going out.

Corporate email systems are an indispensable part of today's business environment but, when misused, can become a major liability for companies. Inappropriate email messages and attachments are putting businesses at higher risk for litigation. Sensitive company intellectual property can find its way out of the company easily. Confidential internal company memos are quickly forwarded to competitors.

In the U.S. securities market, industry regulations from the Financial Industry Regulatory Authority (FINRA) and New York Stock Exchange (NYSE) require a system to be established and maintained to supervise activities of all registered representatives, including their use of email. Written procedures developed for the review of any electronic correspondence with the public relating to investment banking, securities business, and financial advisors must be supported by efficient monitoring and review tools. This requirement places a huge responsibility on the company to track and monitor all incoming and outgoing communications from their registered representatives.

Major reasons for email monitoring include the need to:

- Meet governmental regulatory requirements
- Lower competitive risk by protecting intellectual property such as source code, new product description and theory of execution, formulas, trade secrets, and business processes
- Maintain the company's professional reputation and image
- Maintain employee productivity
- Discourage and prevent sexual or other illegal workplace harassment

- Avoid copyright and other intellectual property infringement from employees illegally downloading software, music, etc.

The Mimosa NearPoint™ Content Monitoring Option provides a powerful, easy-to-use monitoring and workflow solution that you can count on to meet your internal governance and regulatory obligations.

Key Features:

- Custodian's mailboxes are monitored for specific content in real-time
- Ability to create highly granular monitoring policies with an easy-to-use policy creation wizard
- Simple, common-sense reviewer's interface for quick review
- Customizable keyword lists allow for the creation of lexicons
- Comprehensive reporting and logging for audit purposes
- Scalability to thousands of reviewers and millions of messages daily
- Immediate email alerts prompt the auditor or manager to review the questionable content verses remembering to check for alerts every day manually

Key Benefits:

- Lower legal cost and risk—Preemptively identify problems before they become outside litigation
- Protect corporate Intellectual Property and know-how
- Comply with Federal and State monitoring requirements for select industries

CUSTOMER SPOTLIGHT

“Questionable or illegal content in employee email communications has become a major risk for companies of all sizes. The NearPoint Content Monitoring Option enables Corporate Legal and HR departments to proactively monitor their corporate email communications to ensure adherence to their email use policy including the protection of corporate IP.”

— **F. David LaRiviere**
Partner in the Law Firm of
LaRiviere, Grubman & Payne



Live Mailbox Monitoring for Content

FINRA and NYSE 342 specify that each company shall develop procedures for the review of incoming and outgoing electronic correspondence. The Mimosa NearPoint Content Monitoring Option is a powerful, easy-to-use workflow/monitoring application which addresses the FINRA and NYSE regulatory requirements for broker/trader communications monitoring by putting in place policies which compare email and attachment content to a customer defined lexicon.

Powerful Monitoring Policy Creation

The Content Monitoring Policy engine allows creation of very specific requirements for messages to be compared against. These policies can be directed at all mailboxes, geographies, departments, workgroups, specific mailboxes or even specific messages. Built-in message sampling capabilities will also ensure completely random message review policies. Built on the unique capabilities of NearPoint, Content Monitoring can monitor any type of mailbox data—including calendar entries, contacts, tasks, and notes—for policy violations.

Messages and attachments can be scanned for any content including Boolean phrases. A virtually unlimited number of policies can be created to enable granular monitoring. The easy-to-use policy wizard makes creating highly specific policies a quick, straightforward task.

Simplified Reviewer's Interface

Reviewing flagged email messages can be a time-consuming job. The Content Monitoring reviewer's user interface simplifies the reviewing of messages by showing the message content together with the reason for selection by the policy engine. The reviewer is also able to quickly mark the message as compliant or non-compliant and annotate the message with the reviewer's thoughts etc. Messages that have been flagged by more than one policy are only presented once to the reviewer so they do not have to read the same message multiple times. This new interface greatly increases reviewing productivity.

Built-in Workflow Enables Reviewer Workload Sharing and Review

The Content Monitoring Option includes a workflow engine that enables the creation of review groups which allows the sharing of review workloads as well as review deadlines and group reporting.

Creation of Custom Keyword Lists

The Content Monitoring Option matches sampled messages and attachments against a lexicon of keywords or search syntax specified by the administrator. When a message's contents match the lexicon, it can then be marked for review based on policies the administrator has setup.

Comprehensive Reporting

Monitoring regulations specifies each member firm must monitor and show compliance with their adopted procedures, and make those procedures subject to review. The Content Monitoring Option supports these requirements through auditing of supervisor activity and summary reports. Three kinds of reports are available, including Compliance Reports, Review Action Reports, and Policy Reports. The Content Monitoring Option offers many capabilities for customizing reports.

Microsoft®
GOLD CERTIFIED
Partner

DESKTOP REQUIREMENTS

- Microsoft Windows XP SP2
- Microsoft Outlook 2003 SP1

SERVER REQUIREMENTS

- Windows Server 2003 R1, R2
- SQL Server 2000 or 2005 SP1
- Microsoft .NET FrameWork 2.0

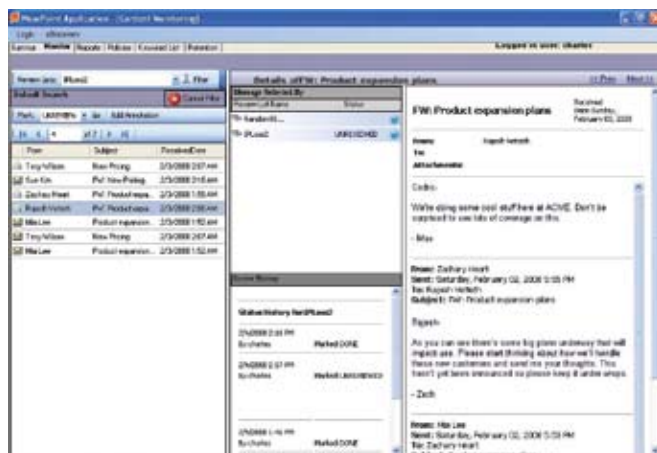


Figure 1. Content Monitoring Option Reviewer's Interface

ABOUT MIMOSA SYSTEMS

Mimosa Systems, Inc., delivers next-generation information management solutions with Mimosa NearPoint, providing a live content archive for Microsoft® Exchange Server. NearPoint unifies archiving, eDiscovery, recovery, and storage management in a single solution, assuring email continuity and regulatory compliance.



Mimosa Systems, Inc.
3200 Coronado Drive
Santa Clara, CA 95054
TEL 408-970-9070
www.mimosasystems.com