

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 inappropriate behavior, e.g. sexual harassment, and other criminal activity. Such 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 ensure 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 put 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.

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 enforcing 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

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



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 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. Additionally, CMO offers many capabilities for customizing reports.



MIMOSA NEARPOINT

SERVER REQUIREMENTS

NearPoint Platform Support

- Microsoft Windows Server 2008 Standard and Enterprise Editions
- Microsoft Windows Server 2003 SP1, SP2—32 and 64-bit Standard and Enterprise Editions
- Microsoft Windows Server 2003 R2 SP1, SP2—32 and 64-bit Standard and Enterprise Editions

Database Support

- SQL Server 2008 Standard and Enterprise Editions
- SQL Server 2005 SP2 Standard and Enterprise Editions

DESKTOP REQUIREMENTS

- Microsoft® Windows XP SP2 or Vista SP1
- Microsoft Outlook 2003 SP1 or later
- Microsoft .NET Framework 3.5 SP1

ABOUT MIMOSA SYSTEMS

Mimosa Systems, Inc. delivers next-generation content archiving solutions for information immediacy, discovery, and continuity. Mimosa NearPoint is the industry's most comprehensive unstructured information management software solution for email, files, and instant messages, enabling archiving, eDiscovery, storage management, and recovery in a unified solution.

MIMOSA SYSTEMS HEADQUARTERS

3200 Coronado Drive
 Santa Clara, CA 95054
 T +1 (408) 970 9070
 F +1 (408) 970 9041
 Email: info@mimosasystems.com

WORLDWIDE OFFICES

Australia +61 (2) 9089 8603
 Canada +1 (613) 797 2952
 China +86 (21) 6103 7361
 France +33 1 55 60 23 62
 Germany +49 (89) 904 7551-0
 India +91 (20) 4048596
 United Kingdom +44 (0) 118 963 7860
 www.mimosasystems.com



FEATURES

Ability to monitor specified users' emails for specific content in real-time

Easy-to-use policy creation wizard to customize highly granular monitoring policies

Simple, common-sense reviewer's interface for quick review

Customizable keyword lists for the creation of lexicons in order to flag matching content

Comprehensive reporting and logging for audit Purposes

Hit highlighting in message body of flagged content

Scalability to thousands of reviewers and millions of messages daily

Immediate email alerts to prompt auditors to review questionable content

Scan and manage sensitive data at rest in the archive, and use SDK to integrate with data loss prevention (DLP) supplier

Deploy easily within the NearPoint platform

BENEFITS

- Comply with federal and state monitoring requirements for select industries

- Save time for compliance offers with a simple interface in which to automate policy enforcement

- Ease review of flagged content by presenting priority content to reviewers in a familiar, simple UI

- Ensure policy enforcement by allowing creation of various keywords and phrases to flag potentially responsive content

- Prove compliance with regulations that require review of certain percentage or samples of content
- Optimize reviewer efficiency by analyzing reports about reviews

- Speed the process of reviewing potentially damaging content by pointing out the specific words and/or phrases that are flagged

- Protect content in even the largest of organizations by automating policy enforcement

- Lower legal cost and risk—preemptively identify problems before they become outside litigation

- Improve security and data loss prevention initiatives by covering both data at rest in the archive via CMO and data in motion via DLP partners
- Strengthen policies by scanning archived data for false positives

- Speed time-to-value with short, easy deployment as CMO is an integrated component of the NearPoint platform