



Trends in Outbound Content Control

A White Paper by Ferris Research

July 2006. Report #636

Ferris Research, Inc.
408 Columbus Ave., Suite 1
San Francisco, Calif. 94133, USA
Phone: +1 (415) 986-1414
Fax: +1 (415) 986-5994
www.ferris.com

Recent Reports From Ferris Research

Reputation Services and Spam Control
Pushing the Limits on Exchange Storage
The Total Cost of Ownership for Voltage Identity-Based Encryption Solutions
Email Archiving Technology Trends
Assessing and Managing the TCO of Mobile Messaging Devices
Mobile Messaging for Exchange: Product Selection and Implementation Issues
Microsoft's Latest Push for Notes and Domino Migration
Snapshot: Lucid8 GOexchange Preventive Maintenance
Exchange Reliability and Its Impact on Organizations
Snapshot: Teneros--Application Continuity Appliance for Microsoft Exchange
Implementing Email Archiving
The Benefits of Integrating Enterprise Content Management Systems and Team Workspaces
Enterprise Mobile Messaging Survey
The Email Archiving Market, 2006-2010
Exchange 12 Assessment
Anti-Spam Technology in the Asia-Pacific Region
Why Exchange 12 Will Be 64-Bit Only
Top 10 Messaging & Collaboration Issues: 2006
The SyncML Standard and Its Impact on Mobile Messaging
Snapshot: Azaleos OneServer
Boundary Email Security: The First Line of Defense
Instant Communications Services and Voice/Video Conferencing
Oracle Content Services: An Alternative to SharePoint Services for Enterprise Content Management
The Plan for AOL Instant Messaging
Snapshot: CipherTrust--IronMail
The Email Security Market, 2005-2010
Techniques for Zero-Hour Virus Protection
New Features and TCO Benefits of IBM Lotus Notes/Domino 7
Introduction to Presence Models and Standards
Proofpoint's Content Security and Regulatory Compliance Offering
Using Content Security to Achieve Regulatory Compliance
Microsoft Operations Manager (MOM) 2005 and Exchange Server 2003 Management Pack for MOM

Table of Contents

Trends in Outbound Content Control	4
Executive Summary	4
What Is Content Control?	4
Key Issues in Outbound Content Control	5
Protecting Corporate Data	5
Complying With Corporate Policy.....	5
Maintaining Customer Confidence	5
Complying With Specific Regulations	5
Managing the Impact of Changing Regulations	6
Preparing for Electronic Discovery	6
Limitations of Current Remediation.....	6
Quarantine of Improper Content	6
Blocking Content	7
Manual Review of Content	7
Deletion of Noncompliant Content	7
Key Trends in Outbound Content Control.....	8
Monitoring Multiple Protocols.....	8
Identifying and Fixing Information Leaks	8
Blocking on Multiple Protocols	8
Extending Control to the End Points.....	9
Reducing Remediation Time.....	9
Monitoring Internal Email.....	9
Beyond Traditional Content Analysis	9
Combining and Reusing Concepts	10
Content-Based Encryption	10
Centralizing Reporting and Administration.....	10
Content Control Solutions from Entrust and Vericept	11

Trends in Outbound Content Control

Executive Summary

Every day organizations create more content, using more types of tools, and share or store that content in more ways than ever before. Content flows in and out of an organization in the form of millions of emails, instant messages, file transfers, and other Internet transactions.

Proactively controlling outbound content mitigates the risk of disclosure and ensures that only appropriate information is sent out in the appropriate way.

The key points of this paper are:

- Businesses are adopting outbound content control for legal compliance, protection against identity theft, and safeguarding of intellectual property.
- Current remediation techniques in outbound content control systems help, but are hampered by a variety of weaknesses.
- Emerging trends in outbound content control include multiprotocol support, improved content analysis, automatic classification capabilities, more selective, content-based encryption, and centralized reporting and administration.

What Is Content Control?

Content control means checking that electronic communications, like emails, instant messages, Web postings, and electronic documents, contain acceptable information. For example, organizations want to ensure that material doesn't contain racial slurs or sexual innuendo, or that valuable product designs aren't being sent to competitors or posted to news groups, or that viruses aren't being transmitted.

Content control needs to take place within an organization. It must also apply to electronic communications coming in from the outside, and to electronic communications that depart the organization for the outside world.

Inbound content control is heavily oriented toward the control of malevolent content, such as viruses, malware, spam control, and denial-of-service attacks. Outbound content control, by contrast, is much more concerned with ensuring that only appropriate material is sent externally; for example, that sensitive material only goes to certain people, or is suppressed entirely.

In this paper, we focus on outbound content control. Because it's of limited importance for outbound control, we ignore the control of malicious content, which also involves largely unrelated technologies.

Outbound content control is a new and important area, with substantial vendor investment. Over the last three years, a range of new types of product have appeared, from such vendors as Entrust, Fidelis, Intrusion, Oakley, Orchestria, Palisade, PortAuthority, Proofpoint, Reconnex, Tablus, Vericept, and Vontu.

Key Issues in Outbound Content Control

Unrestricted release of inappropriate or sensitive information can result in fines, lawsuits, and negative media coverage. Organizations must therefore consider the following issues.

Protecting Corporate Data

Much of the information that an organization creates is proprietary, sensitive, and potentially damaging if improperly released. Corporate financial information, strategic plans, merger and acquisition discussions, earnings reports, records of board meetings, new product details, source code, and customer information are examples of the types of information that should be protected from disclosure.

Protecting the organization's brand, public image, and intellectual assets requires real-time monitoring and analysis of outbound content.

Complying With Corporate Policy

Many corporate policies are not dictated by laws or regulations, nor are they created simply to protect corporate data. These include acceptable use policies, codes of conduct (including harassment, racial slurs, or sexual jokes), ethics and conflict-of-interest policies, and personnel processes.

Maintaining Customer Confidence

Many stories about companies losing customer data appear in the media. New regulations impose strict notification rules on companies that have experienced such a breach. Protecting data is critical for organizations that want to maintain customer relationships.

Complying With Specific Regulations

The most heavily regulated organizations are those in the financial, health-care, insurance, and government sectors. However, legal compliance concerns all organizations whether public or private.

Laws that dictate how U.S. companies should handle data include the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), SEC/NASD rules, the Financial Modernization Act of 1999, and various state consumer protection laws such as California SB 1386. The Companies Act and the Basel II Accord contain disclosure regulations for European companies and all non-European firms doing business with them.

Privacy and identity theft prevention laws require that sensitive customer and employee information be protected from improper disclosure. Such content includes Social Security Numbers (SSNs), credit card numbers, addresses, medical records, and identifying data such as name, email address, birth date, etc.

Managing the Impact of Changing Regulations

Regulations and their interpretations frequently change, forcing companies to constantly update their policies on the handling of sensitive information.

In addition, employees must be trained regarding policies and their updates. This training can take place via email or the company intranet, paper memos, or classroom sessions. Annual security training for employees is obsolete. Now training should be provided more often—even on demand.

Preparing for Electronic Discovery

Whenever an organization is involved in a lawsuit, the process of ediscovery demands that all content related to the matter be found and submitted. Content includes emails, instant messages, fax captures, images of paper memos, and in some situations, digital voice recordings. The ediscovery process is time consuming, labor intensive, and expensive. Companies often find it difficult to locate information in legacy systems and huge message stores. Proper classification and storage help to shorten the ediscovery process.

Limitations of Current Remediation

What typically happens when the content control application detects a profane or harassing email, an unauthorized Web site submission, or a file containing proprietary or confidential information? Most content control implementations use one of four approaches to fixing the problem: quarantine, blocking, review, or deletion.

Quarantine of Improper Content

Typically, a message suspected of containing a virus or information contrary to policy is intercepted and deposited in a special area on the server called “quarantine” pending further action.

A quarantined message, along with any attachments, is given a unique message ID and date stamp. While in quarantine, the item is subject to audit and manual review. At the conclusion of the review process, the message is either released or deleted.

However, quarantining does not provide much analysis of the content and creates excessive false positives, or appropriate emails mistakenly labeled as suspicious. It is also very labor intensive and often stops the flow of legitimate information.

Blocking Content

Blocking suspicious outbound content is the second most common form of remediation. In most systems, blocked content initiates a workflow process that notifies the person(s) responsible for resolving the breach. Periodically, a full, blocked message queue must be cleaned out by email administrators. This method interrupts message flow and may cause legitimate messages to be deleted.

In addition, users typically don't know when they've breached policy or why a message has been quarantined or blocked. Therefore, more advanced analysis of content is advisable, as is user training.

Manual Review of Content

Large enterprise systems amass thousands of quarantined and blocked messages each day. Each message must be viewed and then released, forwarded to an alternative recipient, or deleted. Each type of message (e.g., objectionable jokes or new product plans) may have different people that must be alerted and a different schedule for releasing or deleting it. A manual review process is, therefore, time consuming and often requires extra staff. One large financial institution employs eight people to review quarantined messages. A manual process also inevitably produces inconsistent results as it is a subjective process. For example, one reviewer may release a particular message, while another might delete it.

Deletion of Noncompliant Content

Messages containing blatant violations of policy, such as extreme profanity, are typically deleted automatically without prior manual review or notice to the sender. A log is usually kept of the deleted messages so that they can be reviewed. However, reviewing the contents of any log represents a labor-intensive process. Also, the sender does not know that the message has been deleted or why.

Instead, an automated system should return the errant message to the sender with a link to the company's email policy so the sender can take an alternative action, such as possibly revising the text.

Key Trends in Outbound Content Control

A number of new developments are emerging in the outbound content control area. For example, content control vendors are moving to support a wider range of protocols such as HTTP and IM, in addition to email protocols. They are also extending content control capabilities to file shares and end-user devices.

Along with support for additional protocols, a few content control products include more sophisticated content analysis techniques that go well beyond traditional methods such as keyword matching. These new approaches are helping to reduce the rate of false positives and make content control much more effective and accurate.

Monitoring Multiple Protocols

The content is important, not the particular path it takes. While email over SMTP is the primary way users share content, followed by HTTP and IM, other communication channels and protocols also require attention. Ideally, the same control policy would apply across different media.

FTP and peer-to-peer (P2P) protocols are additional ways users share data, particularly when file sizes exceed the limits imposed on corporate email systems. Since FTP handles very large file sizes and is used by more technically savvy users, FTP is a prime vehicle for releasing source code and design drawings.

Looking ahead, HTTPS, Telnet, Voice over IP (VoIP), videoconferencing, and networked fax represent potential new areas for monitoring and analysis.

Identifying and Fixing Information Leaks

Typically, organizations implement a monitoring system in a passive state for a set period to discover the most prevalent information leaks. Next, they identify the faulty business practices that produced these breaches and work to remedy them.

Most systems enable the organization to create and modify thresholds to fine-tune the content control system. Added benefits of this process are reducing the number of false positives and educating end users.

Blocking on Multiple Protocols

Vendors are starting to support the blocking of content on multiple communication protocols. This is a significant step requiring highly accurate analysis. One common approach is to block content based on the severity of the breach. For example, a file containing two customer records is a registered incident, but a file containing hundreds of records is blocked.

Extending Control to the End Points

Content is often sent from or stored at “end points” such as file shares, desktops, laptops, CDs, USB devices (iPods, memory sticks), and mobile devices.

Organizations are therefore increasingly installing agents on these end points to monitor and block outbound content that violates policies. Agents require more support to deploy, maintain, and synchronize. But they do provide better end-to-end detection and prevention.

Reducing Remediation Time

Once detected, a breach must be quickly resolved. Technologies for doing so have become fairly sophisticated. They can identify the severity level of the breach and send an alert to an IT security manager via an IM client, RSS feed, a monitoring console, or mobile device. They are also adding user-friendly interfaces and approval queues, which enable employees to quickly find and resolve errant content.

Monitoring Internal Email

Due to differences in international privacy laws, multinational organizations are increasingly monitoring content in email traffic among their departments, divisions, and geographic regions.

For example, payroll information can be shared with the finance department, but not with marketing. Or employee information may be shared within U.S. divisions, but not with overseas ones. This sophisticated level of content control involves the creation of role-based policies typically using LDAP or Active Directory.

Beyond Traditional Content Analysis

The problem with analysis techniques in use by most content control systems is that they rely on keyword- and phrase-matching. These methods produce excessive false positives, are difficult to administer, and don't easily scale. They are so focused on exact matches that they often fail to identify the true meaning of the content.

For example, SOX refers to “influential” or “aggressive” language. But note the difference between the sentences “I hate you” and “I hate to see you cry.” Content control systems using a keyword list might flag both sentences, even though the second is clearly not offensive.

New analysis techniques are emerging that use object-oriented approaches to encapsulate content using concepts—also called libraries, categories, or folders. These concepts logically group thousands of search parameters relating to a particular policy.

For example, privacy information within a Personally Identifiable Information (PII) concept group may contain full name, SSN, telephone number, vehicle license plate number, and perhaps educational background and financial data. A HIPAA concept group may contain thousands of medical terms, diseases, and anatomical names.

A more granular analysis focuses on the *context* within the *content* to determine the “attitude” of the subject matter. This is the only accurate way to detect complex concepts like harassment.

Combining and Reusing Concepts

As mentioned above, concept-focused analysis uses categories of related words and phrases to identify broader themes or concepts. Combining two or more of these concepts produces a more effective way to deal with the huge number of suspect messages captured by a content control system.

For example, both the “Earnings” and the “Competitors” concepts might detect as many as 3,000 potential violations each. But, combining these two concepts not only reduces the number of these events, but also shows who in the organization sent earnings information to a competitor.

Concepts can be reused and customized thanks to their built-in inheritance capabilities. Similar to object-oriented programming, lower, or child, concepts inherit characteristics from the parent. For example, the HR, finance, and manufacturing departments share the parent “Identity” concept and set of attributes, then add attributes unique to each department.

Content-Based Encryption

Automated policy-based encryption of outgoing messages is becoming a required component of content control systems.

Automated encryption technologies evaluate outbound content and encrypt and transmit that content according to corporate policy.

Selective encryption should be automatic, performed by the content control solution, and not rely on an end user’s action. For example, if private HIPAA medical data is detected in an outbound email, the system should encrypt it before sending it on without requiring any user action.

Centralizing Reporting and Administration

Typically, using different tools to control content creates problems such as inconsistent reports, unpredictable interactions of different policies, and an extended learning curve. Consolidating content control into one management console enables company policies and business rules to be defined once and pushed out from one location. This reduces implementation and ongoing support costs.

Centralized reporting on protocols, content, and user addresses will help organizations to more accurately identify trends in content flow. Automatic delegation of reports sent to those responsible for a particular concept like “harassment” speeds decision making.

Content Control Solutions from Entrust and Vericept

Entrust and Vericept have entered into a partnership to deliver fully embedded email encryption functionality in a content control solution. Featuring multi-protocol content monitoring and control, the solution mitigates the risk of information breach and protects corporate brands.

Vericept Control 360°, powered by Entrust, features early identification of violations, automatic email encryption, centralized policy enforcement, and reporting. Sensitive emails can be automatically encrypted based on the type of content that is identified, manually encrypted by the end user, or blocked. Automatic enforcement of corporate policies helps to control the flow of information in and out of corporate networks and keeps sensitive information secure.

Benefits of this content control solution are:

- Email encryption can be applied before messages leave an organization.
- Email security processing is done at the server, saving time for users and reducing inbox sizes.
- Email security policies can be centrally managed and automatically applied.
- Email security is not dependent upon users being aware of email encryption techniques.
- Encrypted email can be sent and received via hand-held devices such as RIM BlackBerry.
- Content can be automatically encrypted based on the list of recipients, the nature of the content or in unique circumstances, as dictated by an organization's security policy.
- Flagged messages can also be returned to the user as an educational reminder of company policy. The user can then decide whether or not to send, encrypt or delete the message.

Contact

For further information, visit www.entrust.com. Or contact North America Sales at +1 (888) 690-2424, entrust@entrust.com.

*Author: Nancy Cox
Editor: Sue Hildreth*

Entrust's Sponsorship of This White Paper

Entrust commissioned this white paper with full distribution rights. You may copy or freely reproduce this document provided you disclose authorship and sponsorship and include this notice. Ferris Research independently conducted all research for this document and retained full editorial control.

Ferris Research

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and the Asia-Pacific region.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

Free News Service

Ferris Research publishes a free daily news service. It provides comprehensive coverage of the messaging and collaboration field, and is a great way to keep current. Topics include spam, email, email retention/archiving, mobile messaging devices, consumer messaging services, Web conferencing, email encryption, email migrations and upgrades, regulations compliance, instant messaging, ISP messaging, and team workspaces.

The news is distributed daily. To register, go to www.ferris.com/forms/newsletter_signup.php. In addition, you will receive one or two emails every month announcing new Ferris reports or conferences. To opt out and suppress further email from Ferris Research, click on the opt-out button at the end of each news mailing.