

Reducing the Burden of Administration for Email Content Control, Compliance & Policy Enforcement

Prepared By:

Nemx Software Corporation
14 Poplarwood Avenue
Ottawa, Ontario K2S 1V3
Canada

Table of Contents

Introduction	3
The Challenges of “Policy” Administration	3
The Elements of Policy Definition	4
Policy Management, Maintenance & Administration	4
The Biggest Administrative Headaches	4
Rules-based Implementations.....	4
Rule ≠ Policy — The One to Many Problem	5
Shortcomings of Rules-based Change Management	6
Key Word Based Filters.....	6
Lack of Integration	7
Email Policy Management – A Better Way	7
Integration	7
On-demand Active Directory Integration	7
Seamless Exchange Server Integration	8
Integration with other Email Infrastructure.....	8
Reusability and Independently Managed Policy Elements	8
Self-propagating Change Management.....	9
System Changes.....	9
Policy Changes	9
Hierarchical Policy Management.....	10
Intelligent Content Analysis (ICA)	10
Summary	11

This whitepaper describes the excessive administrative burden associated with "rules-based" email content monitoring and control solutions. An alternative approach based upon independent, reusable elements that provide a hierarchical "policy" management capability without the associated administrative burden is presented.

Introduction

Email compliance, security and content policy enforcement is a growing priority for organizations of all sizes. Many companies have formal policies that govern generally acceptable use and content for corporate email systems. More recently, companies have also become subject to scrutiny and audit to ensure their compliance with a wide range of external regulatory and legal obligations.

However, the mere existence of corporate policies does not ensure compliance. Policies without proactive measures for enforcement are little more than window dressing. Email content control solutions have evolved to provide real-time scanning of inbound, outbound and, in a few cases, internal email traffic. These solutions provide the foundation for proactive, real-time enforcement of regulatory and corporate policies as they pertain to email content.

The single most important benefit delivered by email compliance oriented products is their ability to actually prevent compliance violations from occurring by blocking delivery, or taking some other action on, messages that run afoul of corporate or regulatory policies.

To be effective such systems require:

- 1) a way to embody or interpret corporate policy (such as content criteria or distribution restrictions)
- 2) a method of content analysis to determine whether a particular message does, or with a high degree of probability likely, violate some policy, and
- 3) the real-time ability to take the appropriate action or countermeasure to enforce the policies and thereby prevent violations

Unfortunately, the approach followed by most vendors to implement these capabilities result in a significant, and costly, administrative burden on those responsible for managing the system.

The Challenges of "Policy" Administration

The two biggest challenges that create the administrative nightmare for anyone responsible for managing an email compliance and content control solution are:

- 1) how to define, and reflect within the system, comprehensive and complex corporate policies in a way that preserves flexibility, manageability yet allows for change
- 2) how to define and accurately detect within email messages and their attachments the information concepts that are subject to control under one or more policies

Just because of a "tweak" to my content criteria, or because of a change in personnel, do I really have to manually edit dozens of rules?

There must be an easier way of accounting for plurals, tenses, variations in spelling, use of similar terms and all their possible combinations, than having to create dozens of complex rules myself?

The Elements of Policy Definition

Whether for internal corporate or external regulatory requirements, an effective policy must define three essential elements. They are the:

- 1) *Content* — what kind of information to look for (i.e. confidential information, credit card or account numbers, proprietary product information, financial results, harassing language, etc.)
- 2) *Conditions* — what other restrictions or criteria apply (i.e. when, where, to whom does the policy apply – only to certain recipients or senders, to outbound messages only, etc.)
- 3) *Actions* — what to do if a policy is triggered (i.e. delete the message, quarantine it, encrypt and digitally sign it, copy it, archive it, etc.)

When all three elements are properly defined, combined and represented to the email control system in some way, a “policy” can be enforced.

Policy Management, Maintenance & Administration

The challenges related to maintaining and administering policies for email compliance and control relate to:

- o *the policies themselves* – policies evolve, change and new ones are added. To guarantee proper enforcement the policies must be kept current which may require frequent changes and updates to the system – how often might you have to edit multiple rules simply because of a change in the required action?
- o *defining and fine tuning content definitions* – variously referred to as content filters, key word lists or templates that identify the information that should be detected. Despite advances in technology, to some degree false positive and false negative detections will always be a fact of life—more so with some products and approaches than others, but no system is totally immune. The policy content definitions, therefore, require constant fine tuning and adjustment to improve their accuracy. In addition, customized or personalized filters (i.e. those not supplied by the vendor) often require adjustment over time to tune the results they generate to more precisely match the policy criteria – how many times have you had edit key word lists in dozens of rules to fine tune the results or add additional criteria?
- o *changes in the business environment* – changes in personnel, individual responsibilities, organizational structure, business processes and a myriad of other possibilities all contribute to the administrative burden of managing an email control and compliance system. For instance, a simple change in personnel may mean dozens of policies must be updated to change where policy violation notifications or copies of messages are sent.

Given all the dynamics in the typical workplace, the old phrase “the only constant is change” is apropos when it comes to maintaining the effectiveness and performance of most email control and compliance solutions. The level of time, effort and cost associated with system administration and maintenance can be substantial and in most organizations it often falls on the shoulders of the Exchange or network administrator to perform these administrative tasks.

The Biggest Administrative Headaches

Rules-based Implementations

A rules-based model is the most common approach for defining and implementing corporate email control policies. Unfortunately, it is an approach that adds tremendously to the administrative burden associated with email content control and compliance management.

Rule ≠ Policy — The One to Many Problem

One of the problems with a rules-based approach is that rules are typically simplistic and very one dimensional. Policies, by contrast, can be quite complex and multi-dimensional. For instance, the policy concerning corporate financial data may state that 'financial reports may not be sent to any external recipient except for the company's bank representative(s), the board of directors, the accounting/auditing firm representative(s), and the company's law firm, and then only if the sender is the CFO, Controller or President.' In addition, 'if sent to a valid external recipient the message and any attachments must be encrypted.' It may further state 'internal distribution is restricted to employees in the finance department and senior executives.' Finally, the policy may specify that 'any attempted delivery that violates the policy should result in a notification to the CFO.'

It is virtually impossible to encompass all the aspects of this policy within a single "rule." Multiple rules would have to be defined and may look something like:¹

Rule #1

IF 'financial statement' OR 'financial report' or 'annual report' CONTAINED in 'Subject' OR 'Message Text' AND 'Sender ≠ emailCFO OR emailPres OR emailController' AND 'Recipient ≠ *@companydomain.com' then 'BLOCK DELIVERY'

Rule #2

IF 'financial statement' OR 'financial report' or 'annual report' CONTAINED in 'Subject' OR 'Message Text' AND 'Sender = emailCFO OR emailPres OR emailController' AND 'Recipient = emailBanker OR emailLawyer OR emailDirector OR emailAccountant' 'ENCRYPT and DELIVER' message

Rule #3

IF 'financial statement' OR 'financial report' or 'annual report' CONTAINED in 'Subject' OR 'Message Text' AND 'Sender belongs to Finance Dept OR Executive Group' AND 'Recipient belongs to Finance Dept OR Executive Group' DELIVER message

Rule #4

IF 'financial statement' OR 'financial report' or 'annual report' CONTAINED in 'Subject' OR 'Message Text' AND 'Sender does NOT belong to Finance Dept OR Executive Group' OR 'Recipient does NOT belong to Finance Dept OR Executive Group' then 'BLOCK DELIVERY' AND 'NOTIFY emailCFO'

As this simple example illustrates accurately and comprehensively representing even a single corporate policy can be a complex and time consuming task with a rules-based approach. Any organization with even a modest number of compliance-oriented policies will quickly generate an unwieldy number of individual rules.

Many products attempt to mask the complexity and shortcomings of rule development by providing a Rule Wizard or quasi-graphical user interface. While these wizards succeed in simplifying the actual task associated with defining rules the real administrative burden – the ongoing maintenance, management and configuration of the literally hundreds and even thousands of rules generated – remains an expensive, time-consuming manual effort.

¹ The rules shown here are expressed in a manner to be easily understood by the reader, the syntax used may be similar but does not necessarily accurately reflect the actual syntax of any given rules-based product.

Shortcomings of Rules-based Change Management

Rules, as implemented in most solutions, are designed to be discrete, self-contained individual entities. That is, a rule must encompass all the elements of a policy—content criteria, conditions and actions—within itself.

This approach may simplify rule creation but it adds immensely to the cost and administrative burden associated with change and policy management. A change to the definition or criteria of any element of a policy requires that every rule containing that particular element be manually updated.

For example, you have various policies established and one of the actions for those policies is to send a copy of the triggering message to joe@yourcompany.com. You have a couple of dozen or so such policies so you likely have hundred's of rules as a result. Now suppose Joe leaves the company and all these copies have to be sent to Fran. Someone must now manually locate every rule with an action of "copy to Joe" and change that action and destination address to 'copy to Fran@yourcompany.com'

Its easy to see how quickly and easily the administrative burden can grow exponentially just to keep up with common day-to-day occurrences.

Key Word Based Filters

As we've stated earlier, no system is completely immune to the problem of false positives or, worse yet, false negatives (because you may not even know they are happening!). So content analysis capabilities are not only crucial to detection accuracy but the greater the accuracy the less time and effort that's required administratively to review quarantined messages and tune, add or change content filter lists.

Just as most email control solutions rely on rules, they also rely on simple key words and phrases to identify the content you are looking for. The pitfalls of using key word/phrases for content analysis are many and significant – and the subject of another whitepaper ([Effective Content Analysis for Email Inspection & Control](#) – click the title to download).

Here's a straightforward illustration based on our original example above, after a while you discover that your rules are not detecting all the emails concerning your financial reports and you determine you need to add 'financial results' and 'company results' to the list of content criteria. Even in the simple example above this means going back and manually updating not one but four individual rules to add the new criteria to each one.

Now consider how difficult it is in the first place to create content filters or key word lists that generate accurate results and minimize false positive and negative detections. There are over 30,000

Imagine trying to include all the possible plurals, combinations, tenses, permutations, spelling variations and synonyms your users might choose to use from the 30,000 commonly used words in the English language!

commonly used words in the English language. Can you even imagine trying to include all the possible combinations, permutations, plurals, tenses, spelling variations and synonyms that will capture the real context of what you're looking for and accurately and comprehensively detect all occurrences given the thousands of different ways your users might express themselves?

Even if you diligently build a very comprehensive content filter list, then you have to do it again, and again, and again... for every individual rule that needs to use it. Sure, some of those rule wizards may let you copy an existing rule as a starting point but you still need to add all the other rule elements to it, and don't forget, making any change to that content filter you spent so much time developing involves 100's of edits to all the individual rules that may be using it!

Lack of Integration

Surprisingly few email control solutions offer any substantial integration with the corporate email systems and infrastructure. Appliance-based products, for instance, are often completely divorced from the Exchange email system and its related infrastructure like Active Directory (AD). Many of these products require that you replicate the information you've already invested in developing within Active Directory into their own proprietary structures within their product. Even when such systems support downloading this information from AD there remains the concern and issue of maintaining synchronization as changes are made.

Maintaining the integrity of any information stored multiple times in multiple places (whether its user info in AD and elsewhere or multiple occurrences of the same content filter in many different rules) is always an administrative challenge and time-consuming, costly task.

Some how the "store once" philosophy so prevalent in data management hasn't quite made it into the email control and management world.

Email Policy Management – A Better Way

There has to be a better way to implement and perform email content control and policy administration and management — and there is! What would make policy administration and management easier and less burdensome? These five characteristics:

1. Integration
2. Reusability and Independent Management of Policy Elements
3. Self-propagating Change Management
4. Hierarchical Policy Structure
5. Intelligent Content Analysis

Any product that incorporates these five features will dramatically reduce the effort, time and cost required for administration and policy management.

Integration

Integration can take many forms, described here are those that most directly reduce the level of effort required for the operation of and to maintain and administer email-related compliance and control policies.

On-demand Active Directory Integration

Preserve the investment you have made in Active Directory and eliminate replication, whether done manually or by an automated process, by directly accessing the data in AD when and as needed. This real-time, on-demand approach eliminates any need to duplicate and maintain synchronization of AD-like data in multiple locations.

Moreover, if policy conditions (such as the previous example of restricting messages between users in the finance department) can reference AD Groups, directory lists and individuals then updates made in AD are instantaneously reflected in the email control system. Add a new employee to the finance group in AD and they are automatically subject to the relevant policies with absolutely no change required to the actual policy item – now that's effortless!

Seamless Exchange Server Integration

The more tightly integrated your email content control solution is to your Exchange Server email environment the less additional training and administration is required. In most organizations the responsibility for implementation and administration of the email control system falls to the Exchange or network administrator. To the extent that they can use tools they are already familiar with to perform configuration and administration tasks the more quickly and easily they will be able to complete them.

Since most other aspects of Exchange and the email system are managed from the Exchange System Manager using this tool for configuration and administration of the email content control system as well will reduce the learning curve and increase productivity of your valuable technical resources.

Integration with other Email Infrastructure

Some companies have very large, complex Exchange environments supporting cluster configurations and distributed Exchange servers. Certainly most email control solutions offer multiple server and cluster support but there is significant divergence in how they manage the additional administrative burden associated with these more complex environments.

A centralized system, configuration and policy management approach is ideal. If the email control solution stores its configuration and policy data in Active Directory (without making any schema changes of course) then centrally managed updates to configuration and policy definitions can be automatically propagated to all other Exchange Servers without manually having to copy them to each server.

Some email control solutions support policy-driven email encryption. For those systems if they are also integrated with Microsoft's Certificate Authority they can dramatically reduce the effort and costs related to certificate and key life cycle management. Advanced capabilities should include "auto-discovery" of existing user certificates/keys if they are stored anywhere in the Exchange message store.

Reusability and Independently Managed Policy Elements

We identified that one of the biggest drawbacks to a rules-based approach is the fact that each and every rule is totally self-contained and content definitions, conditions and actions are repeatedly defined in each rule.

A more useful and elegant approach is to separate the policy elements – content, conditions and actions – and define and manage them independently. Using this method actual policy items are established by combining the pre-defined elements. A key benefit of this policy management model is that it supports reusability of policy elements. It also supports self-propagating change rollups as discussed in the next section.

With a true policy (rather than rule) management approach like this generic and specialized actions can be defined independently. Content filters or templates can also be separately defined. Thus a single content template, or combination of several templates, can be created to define the "concept" of 'confidential financial information.' Several different policies may be concerned with restricting confidential financial data but may have different conditions or actions associated with them. Rather than recreating numerous individual rules, as in our earlier example, the use of independent, reusable elements supports the simple "selection" of these common or shared policy elements to 'associate' them with any given policy item.

The advantage of this approach is, of course, that when policy elements are independent entities that are defined and stored only once, then "associated" to one or more policy items, administratively when the need arises to change a content or an action definition you need only make the change once

to the appropriate element. To illustrate the point, in our financial data example, instead of manually updating four separate rules with the exact same change for each one, you just make one change to the single "financial data" content definition that exists. Since all of the policy items related to financial control simply "reference" this single definition once you make the change to the definition ALL policies are instantly updated without having to change them.

Self-propagating Change Management

There are two dimensions to change management and both have been alluded to earlier. One aspect relates to changes to actual system configuration, the other to policy changes.

System Changes

This was briefly discussed in the section on Infrastructure Integration. When a content control and email compliance system is highly integrated with the corporate email system (Microsoft Exchange for the vast majority of companies) typical system configuration and other administration tasks can be minimized.

Storing system setup and configuration information in a way that leverages the existing Microsoft infrastructure so that multiple servers are automatically updated is a good way to lessen the burden on technical resources.

Policy Changes

The more beneficial impact of self-propagating changes is as it applies to ongoing policy administration. A few brief examples highlight the benefits.

One of the most administratively intensive and expensive aspects of any email control solution is management of the content definitions. When content definitions are reusable and independent of any particular rules they become substantially easier to maintain. A typical corporate environment may have dozens even hundreds of policies that deal with the same or similar subject matter. Now if that subject matter is thought of as an "information concept" and that concept is expressed in a single content template (that may itself relate to several sub-concepts) and it is this template that those 100's of policies refer to, then updating those 100's of policies is as simple as changing that single template.

Compare that to manually finding and updating 100's of rules for every change you need to make!

Likewise, if actions are defined and stored separately then applied to a given policy similar savings in time and administrative expense are realized. An action to 'quarantine' triggered messages to the compliance officer, for instance, can quickly and easily be configured. In many organizations any policy violation triggers a quarantine action so many, many policies could include this action. At some future date if there is a personnel change or a change in responsibilities that require that quarantined messages be directed to someone else, effecting this change is as simple as modifying the quarantine action definition to send the messages to the new person's email address. That's all there is to it, once more, there's no manual updating of thousands of policies.

A final example that illustrates how integration has multiple benefits. Various policies may only be applicable to certain groups, individuals or departments. When an email control solution is tightly integrated, with Exchange and AD for instance, it benefits from a level of "organizational" awareness. When policies can be applied to AD Groups or Distribution Lists (instead of specifying a myriad of individuals or addresses in a rule) then any changes made in AD are automatically reflected in the applicable policies. Adding and removing employees, changing which Groups they belong to and any other similar changes in AD will automatically make them subject to the appropriate email control policies with absolutely no changes required to those email policies.

Hierarchical Policy Management

Rules-based systems are very flat in structure. They do not support reusable elements and conflicts can easily arise when attempting to combine rules. In short, its not a very granular or flexible approach.

Another advantage of independent, reusable policy elements is that this structure supports a hierarchical approach to policy management. For example, separate content templates can be created that define sexually harassing language, racially harassing language, discriminatory language, cursing and bullying. When appropriate any individual template can be associated with a particular policy. However, they can also be nested and combined using Boolean logic to create a super template or policy for "offensive language."

A hierarchical policy structure provides more flexibility to easily accommodate exceptions as well. Recall in our first example that executives were allowed to financial information externally. In a system supporting a hierarchical policy structure instead of multiple individual rules a single policy can be defined and in the "conditions" an exclusion or inclusion specified, such that the policy restricting external delivery of financial data "excludes" the Executive group.

Intelligent Content Analysis (ICA)

Intelligent content analysis is an important benefit in and of itself. Obviously, it improves the accuracy of all detection operations and this minimizes annoying, and sometimes costly, false positives and negatives.

ICA also makes a strong contribution to the elimination of tedious, time consuming administrative tasks particularly in the context of content filter or template definitions. It is unrealistic to expect any user, or Exchange Administrator, to anticipate every possible combination of words, phrases or spellings that may be used to express a particular thought or subject. It would be a daunting task to say the least, 30,000 words to choose from and the key words used by many systems only recognize exact matches!

ICA helps solve this problem and reduce by an order of magnitude the administrative effort required. An advanced content analysis engine that incorporates semantic inference and positional analysis needless to say is much more accurate than simply detecting key terms anywhere in a message.

An ICA engine that also incorporates dictionaries, a thesaurus and language processing techniques like root word stemming and expansion and thresholding can virtually eliminate most of the tedious, yet difficult, content filter/template maintenance and tuning most systems require. Instead of looking for just the term "intelligent" an ICA engine, with the features described above, can scan for the 'concept' of intelligence – finding not only the search term intelligent that the user provided, but also, occurrences of smart, clever, bright, intellectual, gifted and so on when used in the proper context.

Benefit #1

Increasing the accuracy of detection reduces false positives and the number of messages quarantined for manual review.

Benefit #2

Instead of tackling the 30,000 word problem yourself, let the system do it for you, automatically

Summary

To dramatically reduce the burden and cost of administration of email content control, compliance and policy management:

- avoid selecting simple rules-based solutions – even those with fancy wizards, they may look good in the beginning, but you'll pay the price later
- look for Policy Management features that support:
 - reusable, independently defined and managed content definitions, conditions and actions
 - hierarchical policy structures
 - automatic, self-propagating change management
- look for a high degree of integration with all aspects of your email infrastructure including Exchange Server, Active Directory and Certificate Authority (if you plan to implement secure mail)
- don't rely on key word lists and filters that need constant maintenance and are often unreliable in terms of accuracy, look for intelligent content analysis that utilizes advanced language processing, semantic inference techniques and dictionary and thesaurus support

Nemx Software Corporation is the leading provider of active email control, compliance and security solutions designed specifically for Microsoft Exchange Server environments. SecurExchange takes the risk out of corporate email by putting you in control of every message – inbound, outbound and your internal messages. With SecurExchange you can:

- Enforce corporate and regulatory compliance, security and acceptable use policies through real-time, policy-driven email inspection and control
- Prevent content compliance violations in email and attachments
- Prevent sensitive information leakage - internally & externally

SecurExchange provides organizations of every size effective, comprehensive and accurate monitoring and enforcement of email compliance policies enhancing security, mitigating corporate risk and liability, and safeguarding sensitive or confidential business information.

To learn more about SecurExchange and how it can contribute to your organization's email compliance efforts visit Nemx at www.nemx.com, email us at info@nemx.com or call us at (613) 831-2010 x230.

SecurExchange
Total E-mail Peace of Mind™