

WHITE
PAPER

Sendmail
Advanced
Anti-Spam Filter

A Unique Approach to Email Policy Enforcement



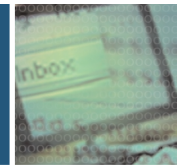
TABLE OF CONTENTS

Sendmail Advanced Anti-Spam Filter

Executive Summary	2
Why Email Policy Enforcement is Needed	2
Overview of Sendmail Advanced Anti-Spam Filter	3
How Sendmail Advanced Anti-Spam Filter Works	4
Unique Content Filtering Technology	4
Source of Email	4
Policy-based Approach	4
Filters and Language Definition	6
Pre-defined Spam Filter	6
Pre-defined Offensive Language Filter	6
Spam Detection and Email Analysis	6
Spam Detection	6
Full Text Analysis Technologies	7
Full Text Analysis Advantages	8
Inspection Process	8
Actions	9
Reporting & Graphing	9
Applying Sendmail Advanced Anti-Spam Filter to a Business Issue	10
How Big Enterprise, Inc. Protects Confidential Data	10
Conclusion	12
About Sendmail, Inc.	12



SENDMAIL®
THE FULL POWER OF EMAIL



This white paper details the requirements for email policy enforcement, describes the elements of a comprehensive filtering system and presents the benefits of Sendmail's email policy enforcement solutions. This document—intended for IT managers, system administrators and CIOs—also examines the business considerations in planning and implementing a policy-based approach to managing the content flowing into, out of and throughout their email systems.

Why Email Policy Enforcement is Needed

Organizations worldwide have come to depend on email as a mission-critical application. Email vastly improves the communication process with co-workers, vendors and suppliers; enables web-based customer support; and gives organizations the ability to disseminate vital information to a global audience almost instantaneously. While the fast, efficient and inexpensive nature of email gives end-users the ability to reach an incredibly large audience, organizations must take steps to proactively manage the content flowing into, out of and throughout their email systems. Failing to take control of employee email can result in exposure to the following risks:

Proliferation of spam — Unsolicited email or junk mail, known as spam, increases network congestion, consumes valuable disk space and diverts employees' attention. The volume of spam has continually increased over the past several years, and that trend is expected to continue—thereby straining an organization's network resources.

Loss of confidential or sensitive data — Sensitive information concerning proprietary technology, corporate strategy, trade secrets or financial data can easily find its way into an outbound email and to a competitor, whether through intentional efforts by an end-user or through unintentional means. (Example: The user accidentally hits "Reply All" rather than "Reply.")

Negative impact on corporate image — Organizations must realize that outbound email can be regarded as an official communication (i.e., sent on 'electronic letterhead') and, when used inappropriately by end-users, can deliver a severe blow to an organization's reputation.

Legal liability — Because many end-users treat email as casual conversation, emails often contain off-color, offensive or inappropriate material. The transmission of a single offensive email can initiate a long and expensive litigation process for an organization and also severely damage its reputation.

Loss of employee productivity — End-users often consider corporate email to be a personal communication tool, and spend a large amount of time sending and receiving non-work-related information, such as jokes, electronic greeting cards, audio and video files and chain letters. This impacts the productivity of the organization.

Degradation of network performance — Large volumes of emails containing attachments (many not work-related) can severely impact the performance of an organization's Internet connection, as well as obstruct transmission of true business-critical traffic.

Exposure to virus threats — The widespread use of the Internet and rapid spread of complex viruses via email have created security issues for organizations of all sizes. Infected emails can be broadcast to entire corporate networks through gateways and mail servers, thereby halting mission-critical business processes.

To mitigate these risks, organizations must introduce an Internet Usage Policy and deploy Policy Enforcement software to monitor and enforce it. An Internet Usage Policy clearly outlines the appropriate uses of email, while Policy Enforcement software inspects the content of electronic communications and takes appropriate action. With the proper Internet Usage Policy and Policy Enforcement software in place, an organization can effectively address the various risks associated with electronic communications and ensure a safe and productive workplace.

Overview of Sendmail Advanced Anti-Spam Filter

Sendmail Advanced Anti-Spam Filter is the only intelligent email and spam filtering solution that allows your organization to proactively monitor, manage and, if necessary, filter unauthorized inbound, outbound and intra-company email messages. In addition, the Filter allows organizations to enforce their unique email security policies with precision, flexibility and ease. By performing Full Text Analysis via patented and patent-pending technologies, Sendmail Advanced Anti-Spam Filter inspects the actual context of messages and takes appropriate action based on an administrator-defined policy. With Sendmail Advanced Anti-Spam Filter in place, an organization can block spam, prevent confidential data loss, reduce legal liability, increase employee productivity and improve network performance.

Deployed at the email gateway, Sendmail Advanced Anti-Spam Filter provides complete control of any SMTP-based email system including Microsoft Exchange, Lotus Notes and Novell GroupWise. In addition, Sendmail Advanced Anti-Spam Filter offers complete control of all inter-office email (MAPI-based) in Microsoft Exchange V5.5 and 2000 environments. Platforms supported by Sendmail Advanced Anti-Spam Filter include Linux, Solaris and Windows 2000.

Sendmail Advanced Anti-Spam Filter analyzes the entire message including the header, body and attachments. For complete inspection of attachments, it recognizes content by file architecture rather than file extension. For example, the product can identify a spreadsheet regardless of whether the file extension is “.xls.” In addition, Sendmail Advanced Anti-Spam Filter recursively breaks down archived and compressed files to filter original message content.

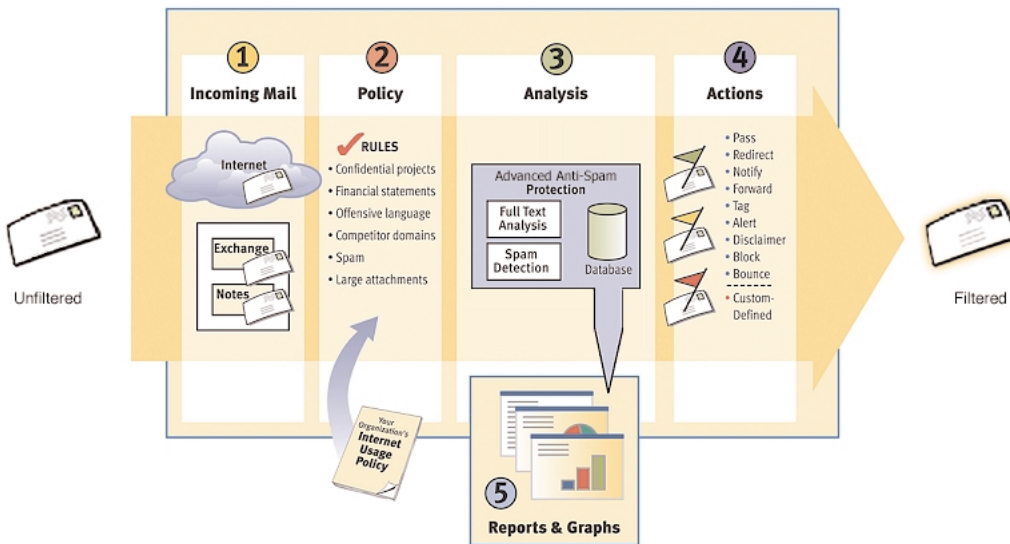
Sendmail Advanced Anti-Spam Filter’s policy-based approach, deployed at the server, offers extreme flexibility in email management and is transparent to the end-user. It provides consistent policy application and effectively manages email by taking actions such as: report, block, redirect the original email to another account, alert administrators or other key personnel, bounce a copy back to the sender, forward a copy, notify the sender or recipient or add a customizable disclaimer. Policy can be defined for individual users, groups, domains or entire organizations.

Based on accurate, detailed data on the use of electronic communications, web-based reports clearly identify policy violators and illustrate usage patterns. Queries can be customized to review activity, and reports allow administrators to view current and archived data both graphically and at a detailed level.

How Sendmail Advanced Anti-Spam Filter Works

Unique Content Filtering Technology

The chart below provides a high-level overview of how Sendmail Advanced Anti-Spam Filter manages email. Beginning with a message entering your organization, each step of the email content and process is outlined. In addition, a detailed description of the technology is provided.



Sendmail Advanced Anti-Spam Filter systematically scans and filters inbound, outbound and intra-company messages for spam and policy enforcement, taking action based on administrator-set rules.

Source of Email

There are three basic sources of email:

Inbound Email — Messages are delivered to an internal server from the Internet.

Outbound Email — Messages are delivered from an internal server to the Internet.

Intra-Company Email — Messages are sent from one internal server/employee to another, that remain behind the firewall.

Sendmail Advanced Anti-Spam Filter can be set to scan all three sources of email.

Policy-based Approach

Sendmail Advanced Anti-Spam Filter provides a policy-based approach to managing electronic communications. This approach provides tremendous flexibility, whereby rules can be aligned with an organization's Internet Usage Policy to specify which messages should be filtered and when, what particular context or attachments should be flagged and what actions should be taken if a policy violation occurs. Sendmail Advanced Anti-Spam Filter installs with a default set of rules that have been determined to be initially useful for a wide variety

of general situations; however, the policy can be quickly customized using a built-in Policy Wizard that guides the administrator through the process of creating new rules. Each rule is defined by the following components:

Name — The administrator names each rule, which clearly identifies the rule's filtering capabilities.

Rank — Every rule has a unique rank, providing a hierarchical system where no conflicts can occur. Rules are applied in rank order with rule #1 applied first.

From — Identifies which user, groups of users or domains are sending the email.

To — Identifies which user, groups of users or domains are receiving the email.

Shift — Rules can apply all the time or only during particular times of the day or days of the week.

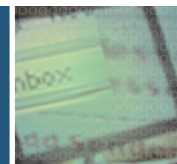
Conditions — Criteria by which the message is inspected, including:

- *The filter(s) containing the desired language content to be identified*
- *Over 200 attachment types including archives, spreadsheets, multimedia, executables and graphics (see below)*
- *Message size*
- *Attachment name (includes wildcard capability)*

Please Note: A combination of criteria can be selected.

Actions — Upon identification of messages that meet the conditions of the rule, actions specify the events that are triggered. Actions are defined using natural language, and suspect messages can trigger multiple events.

File Type Categories	Applications Covered
Archive	.ZIP, .LZH or .tar
Database File	Access, Dbase or Paradox
Email	Body of Email
Executable File	.EXE or .DLL
Graphics File	.BMP, .JPG or .GIF
Multimedia File	.MP3, .AVI or .WAV
Password Protected File	UUENCODE, WinZip, .zip or .tar Archive File
PGP Encrypted Email	Encrypted Email Using the .PGP Protocol
Presentation File	.PPT, .PRE or .PR4
Spreadsheet File	.XLS, 123 or Quattro
Word Processor/Text File	MS Word, Word Perfect and HTML



Filters and Language Definition

Filters identify the particular English language message context of interest and are used during the Full Text Analysis detection process to evaluate email. Sendmail Advanced Anti-Spam Filter provides a hierarchical filter tree structure for greater flexibility and simple management. The filter tree makes it easy to add, modify or delete filters. In addition, each policy rule can utilize a subset of the filter tree, resulting in a “made-to-order” approach to meeting an organization’s policy needs.

Several pre-defined filters are shipped with Sendmail Advanced Anti-Spam Filter. The administrator can edit these filters as well as create new ones. Below is a brief description of these “out-of-the-box” filters.

Pre-defined Spam Filter

To identify and control spam, Sendmail Advanced Anti-Spam Filter provides a highly accurate filter and scalable spam engine. Sendmail Advanced Anti-Spam Filter delivers the highest degree of spam detection and prevention, requiring virtually no administrative attention.

Pre-defined Offensive Language Filter

One of the prominent risks of electronic communications identified earlier is the risk of liability from the use of offensive and inappropriate language. To address this risk, Sendmail’s staff of lexicographic and linguistic experts, in collaboration with a team of professional lexicographers at Oxford University Press (OUP) in England, conducted extensive language recognition research. The result: an extremely comprehensive and accurate categorization of offensive words based on expert standards.

Spam Detection and Email Analysis

Spam Detection

Due to the widespread use of email, organizations must now contend with the proliferation of unsolicited or junk mail, known as spam. Spam places a strain on an organization by degrading network performance, increasing disk space requirements, decreasing user productivity and increasing liability due to inappropriate or objectionable content.

Sendmail Advanced Anti-Spam Filter employs Automated Statistics-based Spam Detection, a patent-pending technology that delivers extremely accurate lexical-based identification of spam (by employing statistical filters that determine the actual content of an email). Once an email has been identified as spam, Sendmail Advanced Anti-Spam Filter invokes the action specified in the policy. The underlying technology consists of:

*A **lexicon*** — a list of characteristic spam expressions, which have been identified by Sendmail’s team of linguistic and lexicographical experts.

*A **database*** — used to determine the statistical “signature” of a spam message. Statistics have been compiled via a training process whereby hundreds of thousands of emails (both spam and legitimate email communications) were analyzed to determine the expected statistical distribution of expressions characteristic of spam.

*A **statistical model*** — quickly analyzes email and uses the database to determine if an email is spam.

Full Text Analysis Technologies

Sendmail Advanced Anti-Spam Filter utilizes Full Text Analysis, an advanced content filtering technique that maximizes detection and minimizes false positives, thereby delivering more accurate results than other filtering approaches. Full Text Analysis integrates a range of techniques adapted from computational linguistics, information retrieval and lexicography into a single, unified solution. Sendmail Advanced Anti-Spam Filter's proprietary Full Text Analysis technologies rely on sophisticated linguistic analysis, which is based on a statistical model that evaluates the frequency of words, co-occurrence of words, uniqueness of words, collocations, morphology and other key attributes. Thus, Sendmail Advanced Anti-Spam Filter understands the characteristics and associations between and among words and how they affect the content and context of a message.

The conventional content filtering technology in competing products is based on a simple keyword or string matching strategy, which may be augmented by Boolean retrieval (including positional operators such as AND, OR, ADJ, NEAR). Because language is inherently ambiguous, the context of words must be evaluated to determine the message's true meaning. Without the ability to analyze the relationship between words, string matching technologies have two primary weaknesses: (1) irrelevant messages are flagged (false positive) and (2) relevant messages are ignored (false negative). These limitations make a string matching approach inadequate. By comparison, two patented technologies—Statistical Dynamic Ranking and Automatic Collocation Identification—give Sendmail Advanced Anti-Spam Filter the leading edge in content filtering. Both rely on statistical modeling, enabling the filter to identify the relevance of the message based on what is specified in the filters. Below are brief descriptions of the key Full Text Analysis technologies:

Automated Statistics-based Spam Detection (patent-pending) — Automatically generates statistical filters to identify specific types of content in electronic communications. Applied to all incoming email, this technique enables extremely accurate identification based on the actual content of the message, as well as other attributes. Spam detection and prevention is highly effective and requires virtually no administrative attention.

Statistical Dynamic Ranking (patent # 6, 119, 114) — Uses advanced statistics to rank documents according to their relevance. Documents are ranked in comparison to other documents that have already been viewed. This technology enables very fine-grained, content-based relative judgments and is a key component of an effective Full Text Analysis implementation.

Automatic Collocation Identification (patent # 6, 173, 298) — Collocational expressions such as idioms and compound nouns ("White House," "affirmative action," "red herring," etc.) are automatically identified and used in the language model. This technology allows collocated words to be evaluated with the special meaning intended by the language, which is another important component of effective Full Text Analysis implementation.

Full Text Analysis Advantages

Full Text Analysis is measurably more accurate than other technologies. The Sendmail Advanced Anti-Spam Filter engine is tuned to maximize detection and minimize false positives. Sendmail Advanced Anti-Spam Filter testing shows a very high accuracy rate.

Other products that use keyword or string matching generate a much higher false positive rate (typically between 25-50%)—which means more work for the administrator to manually “verify” the flagged/suspect messages.

Sendmail Advanced Anti-Spam Filter gives the administrator greater control over the detection process. Because no search technology can deliver a 100% accurate solution, it is critical that the administrator, when needed, be able to take control of the trade-off between flagging all messages that are relevant to a filter (no false negatives but a greater chance of false positives) and flagging only those that are irrelevant (no false positives but a greater chance of false negatives). By allowing the administrator to adjust sensitivity on a filter-by-filter basis (using the sensitivity setting), Sendmail Advanced Anti-Spam Filter delivers an extra level of control, thereby lowering administration costs.

Sendmail Advanced Anti-Spam Filter can be easily configured to deliver high performance in a wide range of environments. Its patent and patent-pending technologies analyze language with minimal burden on the host system—even when processing large amounts of text through multiple filters. Conversely, analyzing the same volume of messages using the string matching approach will bring email traffic to a crawl.

Inspection Process

The following section illustrates how Full Text Analysis technology inspects the message:

- *The email headers are compared against a set of rules that inspect the header for established characteristics of spam, such as missing data in the header. Each rule that applies to the email header raises a flag, and the resulting set of flags provides a signature for the email header.*
- *The statistical model compares the body of an email against the lexicon to determine how frequently each expression in the lexicon occurs in the email. The model analyzes over 300 parameters, including specific language patterns such as \$\$, !!! and phrases such as MAKE CASH FAST. The computed frequencies, along with the additional statistical data contained in the database, result in a score expressing how closely the lexical statistics of the email resemble those of average spam email.*
- *Sendmail Advanced Anti-Spam Filter reviews the “From” header of the email and identifies any known spammer addresses or domains based on a list compiled from sites dedicated to spam control.*

Based on the results of this analysis, Sendmail Advanced Anti-Spam Filter determines if the email’s resemblance to spam is strong enough to classify it as such.

Actions

Depending on the actions specified in the policy rule, the email can be handled a number of ways: pass to recipient(s), block, report, alert administrator, redirect, notify recipient, notify sender, notify user(s), forward a copy, tag as spam, add a disclaimer, bounce a copy back to the sender and dump to file. Multiple actions can be applied to a single message. For example, it may be useful to pass the message to the intended recipient and alert both the System Administrator and the Director of Human Resources that a suspect message has been identified.

Reporting & Graphing

A key part of effective Internet Policy Management software is the ability to provide accurate, detailed data on the use of electronic communications. When an email message triggers a policy rule whose actions specify Report, Sendmail Advanced Anti-Spam Filter enters a record of the event into the database. These records contain information about when the message was detected, the source, destination and message content. Reports are built from records in the database and can be emailed directly to pre-defined recipients. To illustrate usage patterns and identify policy violators, reports contain the following information:

- *Policy rules that were triggered*
- *Content of messages that triggered policy violations*
- *Policy infractions by user and date range*
- *Policy actions taken*

In-depth, web-based reporting, coupled with extensive graphing and charting capabilities, enable organizations to evaluate the performance and effectiveness of their policies at a glance. Graphs illustrate how many messages triggered each rule or underwent each policy action during a specific period of time. Pie charts show the number of policy violations as a percentage of the total number of messages. Below is a description of some of the graphs and charts available through Sendmail Advanced Anti-Spam Filter:

Actions Graph — shows the percent of messages blocked, passed, redirected or tagged as spam

Rules Graph — shows the percent of messages that triggered each rule during a specific period of time

Services by Action — shows, for each service, how many of the messages underwent each policy action during a specific period of time

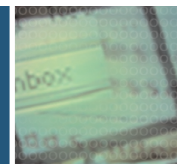
Services by Rule — shows, for each service, how many messages triggered each rule during a specific period of time

Applying Sendmail Advanced Anti-Spam Filter to a Business Issue

The following example illustrates how Sendmail Advanced Anti-Spam Filter can prevent confidential data loss. Because sensitive information is unique to each organization, Sendmail Advanced Anti-Spam Filter's flexible filtering capabilities can be customized to address specific issues such as a merger, acquisition, restructuring, etc. In addition, Sendmail Advanced Anti-Spam Filter provides pre-defined offensive language and spam filters for comprehensive coverage.

How Big Enterprise, Inc. Protects Confidential Data

Big Enterprise, Inc. has a financial team engaged in analyzing Small Company, Inc. as an acquisition candidate. To protect the sensitive nature of this project (coded Project Value), the company monitors email communications. The goal is to prevent information related to "Project Value" from being intentionally or unintentionally sent beyond the acquisition team.



Sendmail Advanced Anti-Spam Filter is deployed on the network of Big Enterprise, Inc. In order to ensure that any messages suspected of containing information related to "Project Value" are detected, a rule is added to Sendmail Advanced Anti-Spam Filter's policy. This rule specifies that Sendmail Advanced Anti-Spam Filter should inspect email going to any address using a newly created filter to detect "Project Value" or acquisition-related content. This rule specifies that any suspect message should be redirected to the appropriate executive for review.

To create the rule, an appropriate filter tree is built first. Within the filters section of Sendmail Advanced Anti-Spam Filter, the "Confidential" filter is defined as a main (high-level) filter—which, in this example, is subdivided into:

Company Language — This filter contains entries of company-wide confidential indicators such as: "company confidential," "do not forward this email," "top secret" and "internal use only."

M&A — This filter contains entries related to mergers and acquisitions. Big Enterprise, Inc. can subdivide the M&A filter into two sub-filters:

- **Generic** — Includes common M&A terms such as "intellectual property," "purchase method," "pooling of interests," "acquire," "business alliance," "investor rights agreement," "controlling interest," "growth rate" and "due diligence."
- **Specific** — Includes identity-specific or common names such as "Small Company, Inc." or "Project Value."

Full Text Analysis employs semantic, contextual and morphological analysis to accurately detect messages relating to the acquisition. By using Full Text Analysis technologies to assess messages with respect to its filters, Sendmail Advanced Anti-Spam Filter provides the following advantages:

Automatically understands collocations — Sendmail Advanced Anti-Spam Filter will detect word combinations such as "intellectual property" as having unique meaning that is very different from when the words are used separately or in conjunction with other words. Full Text Analysis will flag a message such as "the value of the intellectual property" while the message "the property is worth hundreds of dollars, and the new office will provide a sanctuary for all my intellectual pursuits" will not be flagged. As a second example, a filter entry identifying the collocation "terms of the merger agreement" will ensure that when either "merger agreement" or "terms of the agreement" appear in an email, the message will be flagged as suspect.

Automatically considers all the inflections of the words in a filter entry — If the filter entry contains the words "purchase method," an email discussing "several new purchasing methods" will be flagged. In contrast, a document discussing the "Methodist church" will not be flagged. Other technologies might attempt to catch various forms of "method" by requiring the user to write a construct like "method"—which would also retrieve "methodist" or "methodism." The following two examples illustrate the effectiveness of Full Text Analysis technology: the ability to flag generated (but not general) and capitalize (but not capitalism). In addition, Sendmail Advanced Anti-Spam Filter distinguishes "interested" as unique content unrelated to "pooling of interests," although they have the same morphological root.

Every filter entry can be fine-tuned via the sensitivity slider — This tuning provides greater control of the detection process. No search technology can deliver a 100% solution. Moving the slider to a higher sensitivity or lower sensitivity will adjust an entry's default sensitivity setting, providing the administrator with greater control of the trade-off between



false positives and false negatives. In the case of Big Enterprise, Inc., the highly sensitive nature of Project Value requires that every suspect message be flagged and reviewed. Therefore, the “Confidential” filter is set for maximum sensitivity—with the knowledge that a higher number of false positives will result. On the contrary, Big Enterprise considers detecting offensive content a lower priority—so a mid-range sensitivity setting, resulting in fewer false positives and less review for the administrator—is deployed.

Supports thousands of filter file entries — Most categories cannot be summarized in two or three filter entries but require dozens, if not hundreds. Sendmail Advanced Anti-Spam Filter was built from the ground up to support many entries. Sendmail Advanced Anti-Spam Filter is efficient with thousands of entries as well as with only a few dozen, whereas competing products are limited to a very small number.

Allows users to group filter entries into hierarchical filters — This hierarchy provides for greater flexibility and simple management. As a result, each policy rule can employ any portion of the filter tree. In this example, the policy rule will specify the entire confidential filter in order to maximize the protection of highly sensitive information.

This example illustrates how companies, like Big Enterprise, Inc., can easily customize Sendmail Advanced Anti-Spam Filter to meet their specific needs. By utilizing Full Text Analysis, Sendmail Advanced Anti-Spam Filter quickly scans messages to ensure that confidential data is protected and not sent to an inappropriate party.

**CONCLUSION**

Today's business environment requires organizations to address the risks associated with email usage. These risks include the proliferation of spam, the loss of confidential data, potential legal liability, network performance degradation and a reduction in employee productivity. Sendmail Advanced Anti-Spam Filter mitigates these risks by intelligently and proactively monitoring, managing and, if necessary, filtering unauthorized inbound, outbound and intra-company email messages. It provides complete control over the flow of any SMTP-based email system by taking preset actions on messages. In addition, in-depth web-based reports help illustrate usage patterns and identify policy violators. Sendmail Advanced Anti-Spam Filter's policy-based approach offers extreme flexibility and manageability while remaining transparent to end-users.

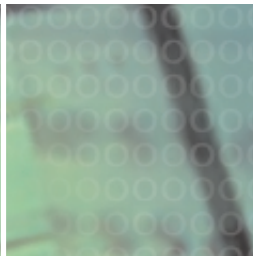
About Sendmail, Inc.

Sendmail offers an email solution that meets the needs of enterprises and service providers for new levels of control, scalability, flexibility and reliability through consolidation of the messaging infrastructure on a single mainframe.

Sendmail provides unprecedented control of the mail stream and of the messaging system, protecting against spam, viruses and intrusion while giving legitimate users secure message access. Sendmail's Policy Enforcement Filters, leveraging the unique API built into the Sendmail MTA, allow comprehensive policy-based control of data passing through the system to limit liability, scan for viruses, protect sensitive data and enable regulatory compliance and policy enforcement. Powerful, intuitive interfaces and tools make installation, configuration and account and data management easy and secure, lowering administrative costs and speeding deployment.

Sendmail is designed for fast, flexible growth, scaling to millions of users at extremely high levels of concurrency—quickly, cost-effectively and without degradation in performance, usability or manageability. Mobile messaging capabilities give users anytime, anywhere access from a diverse collection of devices and interfaces, with a consistent view of messages from any device. Sendmail's standards-based, modular architecture allows flexible integration of heterogeneous messaging environments (including groupware applications) and enables rapid assimilation of new technologies, networks and user bases.

Finally, Sendmail provides reliable, highly available service. Online storage reconfiguration and backup, dynamic data updates, a partitionable message store and powerful technologies keep downtime to a minimum. In the event of failure, robust backup and restore capabilities prevent data loss and enable quick recovery.



WHITE
PAPER
Sendmail
Advanced
Anti-Spam Filter



SENDMAIL®
THE FULL POWER OF EMAIL

Sendmail, Inc.
6425 Christie Avenue, 4th Floor
Emeryville, CA 94608

510 594 5400
www.sendmail.com
sales@sendmail.com

© 2002 Sendmail, Inc. All rights reserved. Sendmail and the Sendmail logo are registered trademarks of Sendmail, Inc. All other trademarks or service marks are the property of their respective companies.

A Unique Approach to Email Policy Enforcement