# Table of Contents

1.0 Introduction............................................................................................................. 3  
1.1 Security Risks over Email and Instant Messaging.............................................. 3  
1.2 The 8300 Series: Single Solution for Multiple Security Risks........................... 3  
2.0 Architecture Overview............................................................................................ 4  
2.1 All-in-one appliance............................................................................................ 4  
2.2 Scanners and Control Center .............................................................................. 4  
2.3 Inbound and Outbound Email Processing........................................................... 5  
2.4 Public IM Security Proxy.................................................................................... 6  
3.0 Comprehensive Threat Protection over Email and IM ........................................... 7  
3.1 The foundation: Symantec Response Technologies and Infrastructure.............. 7  
3.2 The Email Firewall ............................................................................................. 8  
3.3 Spam protection powered by Brightmail .......................................................... 13  
3.4 Email virus and outbreak protection................................................................. 15  
3.5 IM Security ....................................................................................................... 18  
4.0 Content Filtering and Outbound Content Control ................................................ 19  
4.1 Capability Walkthrough: Creating a Compliance Policy .................................. 20  
5.0 Policy and System Management........................................................................... 23  
5.1 Centralized Administration............................................................................... 23  
5.2 Flexible Group-based Policies ........................................................................... 24  
5.3 Reporting........................................................................................................... 25  
5.4 End User Features ............................................................................................. 26  
5.5 System Management Features .......................................................................... 26  
6.0 Further Reading .................................................................................................... 27
1.0 Introduction

1.1 Security Risks over Email and Instant Messaging

Electronic messaging is a key enabling technology that can be leveraged to achieve business benefits. In today’s world of multiple communication protocols and new variants of threats targeted towards messaging systems, securing a corporate messaging environment has never been more challenging.

For most organizations, email represents the single most critical channel for internal and external communication. With the increase in network bandwidth, the use of email as transport for rich media is now common; beyond simple text, email is now used to send rich media including HTML, graphics, audio and video. Having become critical for corporations in the 1990s, email is now growing in its importance as an accepted form of business record.

However, email is not the only means of electronic messaging and collaboration. In the last few years, instant messaging (IM) has been rapidly adopted in many organizational settings. Users in most organizations now use IM, even if the IM is not yet supported by their IT organizations. It is estimated that IM may even eclipse email by 2008, as measured by the number of messages sent between users. IM protocols have been extended to allow voice and video information transfer.

As with email, the ease and power of IM brings with it a collection of risks and challenges. IM has increasingly become the target for attackers to propagate IM-borne viruses, worms, spam (spam over IM), malware, and phishing attacks. Though widely adopted, IM is generally unprotected and unmonitored in consumer and enterprise environments, leaving it vulnerable to attacks and exploits. These attacks have grown exponentially over the past three years, increasing the need for real-time threat response for IM and peer-to-peer (P2P) applications.

The overall impact of common messaging security threats can be measured in the following ways:

- End user productivity, IT resource, and messaging infrastructure drain due to spam and unwanted email at the gateway
- Asset damage and downtime due to virus attacks and worm outbreaks
- Regulatory and organizational pressure to monitor and control inbound and outbound email content
- The time spent by administrators to deploy and manage a messaging security solution

The ongoing issue facing messaging administrators is how to preserve the value of messaging in light of these escalating security threats. Since they are now occurring over multiple protocols, organizations are seeing an increased need for integrated secure content and threat management solutions that address multiple threats in a single solution.

1.2 The 8300 Series: Single Solution for Multiple Security Risks

The Symantec™ Mail Security 8300 Series appliance is Symantec’s response to the messaging security problem at the gateway. With Version 7.5, the latest system upgrade to the messaging security appliance platform, now have access to the first solution that integrates best of breed email security, IM security, and premium outbound content control capabilities in one appliance. With the 8300 Series, administrators can:

- Stop spam, denial of service attacks, and other inbound email threats using the industry-leading Brightmail Antispam technologies and response capabilities
- Leverage global and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections
- Filter email content to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data leakage over email
- Secure and protect public IM communications using the same management console as email
- Obtain visibility into messaging trends and events with minimal administrative burden

This white paper provides current and prospective 8300 Series customers an overview of the underlying architecture of this gateway based appliance and a walkthrough of the key capabilities of the solution.
2.0 Architecture Overview

The power of the Symantec Mail Security 8300 Series begins with its architecture, gateway-based approach, and easy deployment.

2.1 All-in-one appliance

The Symantec Mail Security 8300 Series is an all-in-one appliance, a deployment model that is becoming the platform of choice to secure the gateway. The 8300 Series integrates the core hardware and software pieces necessary for a comprehensive, secure, and easy-to-deploy messaging security solution. These elements include:

- **Hardware.** The Symantec Mail Security 8300 Series features compact, rack-mounted, Intel®-based server appliances. Based on proven, high-performance, custom-manufactured hardware, the Symantec Mail Security 8300 Series includes standard features such as redundant storage using RAID. A high availability model includes features such as dual power supplies and fans.

- **Software.** A preinstalled Linux®-based operating system powers the Symantec Mail Security 8300 Series. In addition, the filtering and management platform software is resident on the appliance. Also included is an IM relay and all the necessary mail transfer agents (MTAs) that enable email communication with the outside world and with internal mail servers, such as Microsoft® Exchange. Future software updates are easily applied, ensuring minimal disruptions for security updates.

- **Secure configuration.** To mitigate the risk of having email servers directly exposed to the Internet, Symantec Mail Security 8300 Series appliances are backed by a secure platform of technologies. The embedded operating system includes a locked-down kernel and ships pre-hardened against common vulnerabilities and attacks. For example, to prevent exploitation from hackers, only the most vital services are included and all unnecessary ports are closed.

Similarly, the included MTAs are secured against unauthorized relaying and buffer overrun vulnerabilities. Administration and management is also protected by Web-based authentication, allowing access only to authorized users within the organization.

- **Automatic updates.** To ensure comprehensive protection against the latest email threats, the email security defenses are constantly fortified in real time with automatic anti-spam/antispam filters and anti-virus definitions from Symantec. Symantec performs all the filter updates, relieving the administrator of the ongoing administration burden. The filter download process includes two-way validation to guarantee that updated filters and anti-virus definitions are coming from Symantec. Filtering remains in effect even when the appliance is receiving updated filters, so even during updates administrators remain fully protected.

2.2 Scanners and Control Center

Each Symantec Mail Security 8300 Series appliance can be used to perform a variety of functions at a site. For smaller installations, administrators can configure the same appliance to perform all needed functions. Larger installations often choose to deploy numerous appliances to perform specialized functions. The available functions are:

- **Dedicated Scanner.** Performs email filtering or optionally IM filtering. Symantec does not recommend provisioning a Scanner to perform email and IM filtering on one appliance. Administrators can set up one or many Scanner appliances. For load balancing and high availability purposes, multiple SMS 8300 appliances can be configured using round robin DNS and weighted MX records.

- **Dedicated Control Center.** Manages the Scanners at a site. Each Symantec Mail Security 8300 Series installation has exactly one Control Center appliance. The Control Center appliance, which can manage multiple Scanner appliances, also hosts the email spam and suspicious attachment quarantines as well as storage areas for compliance incidents. Note that the Control Center is responsible for functions such as centralized reporting, policy management and message tracking. In the rare event that the Control Center goes offline, the crucial functions of message filtering and delivery continue via the Scanners, which can be easily scaled horizontally.

- **Combined Control Center and Scanner.** Performs both functions. This all-in-one configuration is suitable for smaller installations.

The following figure summarizes the functions of the 8300 Series when deployed as a Scanner and a Control Center.
2.3 Inbound and Outbound Email Processing

When configured for email scanning, Symantec Mail Security Series 8300 Series appliances typically operate at the outermost gateway layer, responsible for processing incoming and outgoing email. For the core messaging platform, the 8300 Series includes a powerful MTA solution, providing the performance, security, and flexibility administrators need. Among the MTA features are per-domain routing, aliasing, and masquerading for senders and recipients.

As depicted in the following figure, mail flowing through the appliance undergoes a number of processing layers and filtering modules. These layers include Email Firewall checks based on the reputation of the source or IP connection, anti-spam filtering using Symantec Brightmail® technology, award-winning Symantec AntiVirus™ protection, content compliance checks, and more. To protect against the latest email threats, the email security defenses are constantly fortified in real time with automatic updates from Symantec. Because Symantec performs all the filter updates, ongoing administration amounts to running reports to validate effectiveness and monitor mail flow. However, if administrators want more flexibility and control, administrators can make use of the suite of available management features. For example, administrators can choose to set up a specific policy for messages identified as spam for different groups of users in an organization.
In today’s world of mixed threat messages and complex regulatory mandates concerning email content, it is crucial to have a comprehensive view into the mail flow at the gateway. For example, a single message could be spam and also contain a virus. Another email could simultaneously trigger multiple different content compliance policies, such as GLBA and acceptable use. First generation solutions that can deliver a single, specific verdict (or disposition) for processed messages introduce vulnerabilities in the system and also provide an incomplete view of filtered traffic at the gateway.

Leveraging next generation Mail flow Analysis, the 8300 Series runs each message through all available modules and collects all applicable dispositions for a message. These dispositions are then fed into the policy engine, where the configured actions are combined and reconciled according to industry best practices. For example, suppose that a spam message also contains a virus. Also suppose that an organization’s security policy specifies that spam messages should be quarantined and that viruses should be cleaned. Instead of cleaning the virus and delivering the spam to user inboxes, Symantec Mail Security cleans the virus and holds the cleaned, spam message in Spam Quarantine. This enhanced Mailflow Analysis feature accomplishes the key goals of reporting and acting upon multiple dispositions per recipient without performance penalties. For this release, the combination and conflict resolution occurs requires no administrator intervention.

From a deployment perspective, 8300 Series appliances are designed to reside at the perimeter of the email network, serving as a protective layer in front of existing email servers located downstream in the network. The filtering Scanners are often deployed in the demilitarized zone (DMZ) in the network, whereas the Control Center appliance will be behind the more restricted internal corporate firewall.

For larger installations, administrators can easily scale a Symantec Mail Security 8300 Series deployment by adding additional Scanner appliances that are managed by one Control Center appliance. In this scenario, the Scanner appliances serve as the gateway MTAs, processing inbound mail and relaying it to other messaging layers or to the groupware server. Figure 3 shows an example of such a multisite deployment, connected over a wide area network (WAN). This scenario in Figure 3 can be further optimized for performance by modifying the roles for the Scanners. For example, at each site, administrators can set aside one dedicated scanner for inbound filtering and another for outbound. Administrators optionally dedicate another Scanner for IM filtering and control.

2.4 Public IM Security Proxy

When configured for optional Instant Message filtering, an 8300 Series Scanner acts as a proxy for securing, managing, and logging multiple instant messaging protocols. The 8300 Series software is typically installed on a server behind one or more corporate firewalls.

To control public IM protocols, simple port monitoring is not sufficient because many public IM clients are ‘port crawlers,’ often attempting to connect on multiple ports. However, public IM clients only seek to connect to a very short list of hosts, for example: login.oscar.aol.com and messenger.hotmail.com.

Because of this, the easiest and most thorough way to handle public IM messages is through DNS redirection:

A typical transaction:
1. A user signs onto a public IM client with their screen name and password. During the authentication, the client attempts to connect to the public relay.
2. The local DNS server has several zones for each of the public IM protocols that will forward this request directly to the 8300 Series appliance rather than allowing the client to connect to the internet and directly access the public relay.
3. The 8300 Series ascertains who the user is through screen name registration. 8300 Series then applies all applicable policies to the message (spam filtering, virus scanning, etc…) and logs the message to the data repository.
4. The corporate firewall is configured to block any rogue IM connections that are attempting to bypass the 8300 Series server. Essentially, a firewall policy ensures that the only internal...
machine that can connect to login.oscar.aol.com, or any other public relay, is the 8300 Series server.

This architecture has three key advantages:
1. It requires no client side configuration changes or software installation
2. It is not dependant on inspecting specific ports that a client might circumvent.
3. The 8300 Series is not managing IM conversations through deep packet inspection. So, it is not inline with other internet bound protocols, such as HTTP, SMTP, and FTP.

3.0 Comprehensive Threat Protection over Email and IM

3.1 The foundation: Symantec Response Technologies and Infrastructure

An integral component of the Symantec Mail Security 8300 Series architecture is the unique response infrastructure provided by Symantec. To keep ahead of the latest email security threats, Symantec maintains threat detection and response centers located across the world. These focused and coordinated operations centers, part of Symantec Security Response, operate 24x7 and perform the following vital functions:

- **Real-time email threat monitoring with the Probe Network.** A key asset for Symantec Security Response is the Probe Network, an extensive array of over 2.5 million decoy email addresses, also known as honey pots. This patented global network of email accounts attracts and collects large quantities of spam and related threats—tens of millions of spam messages pass through the Probe Network every day. Symantec uses these decoys to stay current with the latest spamming tactics and detect early stage virus-infected attachments.

- **Virus definitions from Symantec Security Response.** To provide up-to-the-minute, round-the-clock protection, virus protection in the Symantec Mail Security 8300 Series is backed by Symantec Security Response. At Symantec Security Response, the industry’s largest team of experts works to identify and neutralize viruses before they can enter the network and spread across the enterprise. Symantec Security Response provides swift, global response to virus outbreaks and proactive research on future threats.

- **Automated anti-spam filter creation.** Leveraging sophisticated tools, machine learning, and automated processes, Symantec Security Response creates defenses that eradicate current spam attacks and their variants. Using the Probe Network to create filters based on actual spam is what drives the near-perfect accuracy rate for spam filtering. To combat emerging threats and new spam, Symantec Security Response also develops, tunes, and deploys other more proactive filters, such as heuristic-based filters. The Symantec Mail Security 8300 series architecture represents a constant feedback loop, starting and ending with the customer site:
  1. At the customer site, the Scanner appliance executes filters based on up-to-date protection from Symantec Security Response.
  2. The Scanner constantly reports back to Symantec Security Response regarding the effectiveness of deployed filters. If necessary, adjustments are made in real time by Symantec Security Response to improve effectiveness.
  3. Users at the customer site can choose to easily submit missed spam messages to Symantec, increasing the breadth and reach of the Probe Network with the click of a button.

The following figure summarizes the scope and coverage of Symantec’s Email Security Group.
• **IM Threat Center.** The 8300 Series integrates with the Symantec IM Security Threat Center for auto-updates of virus, worm, and spam definitions, and for connectivity to the real-time threat protection service (RTTPS). RTTPS is a proactive filtering system for detecting, deflecting and eliminating malicious content sent through IM. RTTPS features a traffic filter that watches for anomalies or patterns that could signal the work of a virus, such as rapid-fire sending of messages. It also looks at content and embedded links, and scores them against a reputation engine. Using auto-updates, 8300 Series will periodically call the Threat Center to pull the latest list of malware definitions, worm signatures, and spam signatures to each local deployment. Additionally, RTTPS will receive high priority threat information from the global RTTPS community and the Threat Center. This threat information and worm signatures will be automatically sent to 8300 Series to block any suspicious activity in the environment. Any malicious content signatures will be analyzed by the Symantec Mail Security Threat Center to validate and confirm the behavior is associated with a known or new outbreak.

• **Deployment of timely defenses.** Approximately every 10 minutes, updated anti-spam filters and other email security defenses are pulled down over a secure connection to Scanner appliances at the customer site, where the filters are immediately put into action. For timely, round-the-clock protection against rapidly spreading, destructive viruses, updated suspicious virus definitions flow to customer sites using the same secure mechanism that transmits anti-spam filters and reputation data.

### 3.2 The Email Firewall

A solid combination of anti-spam and anti-virus protection is just one part of a comprehensive email security solution. For numerous reasons, an email security solution must also be able to reduce unnecessary incoming email traffic. First, scanning email for spam and viruses is an inherently resource-intensive task, impacting CPU and other resources as the message content is scanned. Any mail that must be processed past the gateway measurably impacts the email infrastructure, capacity of resources, and the quality of service for mail.

Stopping potential attacks is another reason to ensure that certain mail doesn’t breach the gateway in the first place. A representative example is the directory harvest attack, an abusive tactic that results in huge levels of email volume and compromises an organization’s email directory information. In these attacks, spammers send thousands of empty messages to mail servers in order to obtain legitimate email addresses. By tracking which addresses are not rejected, they can determine valid email addresses to be used in future spam or phishing campaigns.

The best email security solutions accurately reject unwanted mail at the gateway based on its IP address. Such SMTP connection management features are an increasingly effective method of dealing with the side effects of increased email volume. Where many competing SMTP connection management approaches miss the mark is in their poor quality of sender information used to block connections. And
worse, they often result in blocking legitimate traffic. In order for any connection management approach to precisely and reliably identify good and bad email senders, it must have access to a large stream of email sender data.

Symantec Mail Security 8300 Series features the Email Firewall, a set of automated and configurable connection management features that go into effect as soon as an incoming connection is detected. A first level of defense, the Email Firewall serves as a “gatekeeper” in front of the more CPU-intensive pieces of the filtering engine, including the anti-spam and anti-virus layers. It can be automatically configured to block spam attacks, directory harvest attacks, connections from senders identified as spammers by Symantec, and more. By leveraging its Probe Network of decoy email accounts and the filtering statistics over its 450-million user anti-spam customer base, Symantec is in a unique position to accurately characterize email sources.

The Email Firewall is the first stage in the inbound protection process. It protects the internal infrastructure by detecting and examining the incoming IP connection before the gateway mail server in the 8300 Series accepts a message. It can then take preventative action such as SMTP connection management or throttling. The Email Firewall also recognizes and blocks directory harvest attacks and denial of service attacks.

Why is it important to have defenses at the connection level? After a brief slow-down in 2005, customers are reporting that spam volumes are surging to unprecedented levels. This increase is straining customer email infrastructures as email scanners are processing more messages unnecessarily. Filtering mail for spam and viruses slows down email delivery and taxes CPU and mail server resources because each message needs to be opened and processed. As a result of the increased volume of mail at the gateway, organizations are forced to buy additional email gateway systems and groupware servers. The Email Firewall detects undesirable connections and blocks or defers them, restoring valuable filtering cycles to the Scanner.

### 3.2.1 SMTP traffic shaping using Local Reputation

Spammers routinely leverage vast networks of compromised client machines—botnets—to disseminate their attacks. This low volume, highly distributed approach enables spammers to generate huge quantities of messages yet also stay under the radar of global “Sender” reputation lists that generally aggregate dozens third party DNS black lists and tend to naturally focus on high volume senders.

SMTP traffic shaping is an Email Firewall tool to tackle the problem of escalating email volumes. It also provides stronger defenses against the botnet-driven spam. The feature was designed to eliminate 50% of incoming messages from being filtered. The following figure shows the dramatic up front reduction in spam witnessed by a Symantec customer who enabled SMTP traffic shaping:

<table>
<thead>
<tr>
<th>Messages Seen daily</th>
<th>700,000</th>
<th>600,000</th>
<th>500,000</th>
<th>400,000</th>
<th>300,000</th>
<th>200,000</th>
<th>100,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/31/2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/7/2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/14/2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/21/2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/28/2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SMTP Traffic Shaping set to High**

**Spam Reduction Results**
- 50% (average): Removed at MTA level by SMTP Traffic Shaping
- 45% Caught with full scanning
SMTP Traffic Shaping works by tracking the local reputation of IP connections that are connecting to a given scanner at a customer site. Based on the data that it collects, the appliance can slow connections (with SMTP deferrals) from sources that are known to send spam before the messages enter the appliance and are processed by the Scanner. This reduces load on the Scanner appliance(s) and improves the performance of the system. The local reputation database is constantly updated based on sender behavior. Senders with a clean history receive a better quality of service than those with poor records. Similarly, an IP address with a poor reputation can improve its reputation score over time by sending less spam and more legitimate mail.

The key benefit is the configuration simplicity. Instead of complex score management and maintenance, administrators simply select the aggressiveness setting: high, medium, or low. Behind the scenes, the Scanners use a probabilistic algorithm to defer or allow the connection. Symantec can mitigate false positives by relying on the native retry capabilities of most legitimate remote SMTP servers (unlike legitimate mail servers, most zombies respond to deferral attempts by moving on to the next target in their list).

From a deployment perspective, note that SMTP Traffic Shaping:

- Works only if the SMS appliance is the first hop at the email gateway. If the Scanner cannot evaluate the raw source IP, it won’t be able to accurately classify the remote host.
- Leverages local reputation verdicts only. The analysis does not incorporate global reputation data from Symantec’s downloadable proprietary reputation lists or optional DNS-based third party lists. Administrators set up those services elsewhere, in the Sender Groups section of spam protection configuration.
- Continues to record sender reputation information even when this feature is disabled. This means that administrators can disable this feature temporarily and not miss any sender data during that time.

3.2.2 Directory harvest attacks protection

The Email Firewall can also examine, detect, and mitigate possible directory harvest attacks. In these attacks, spammers launch a program that sends thousands of messages to dictionary-generated email addresses within a company’s domain. The sender’s goal is to monitor how the mail server rejects requests for recipient email addresses that don’t exist. This feedback from the server provides the spammer with the information he needs—valid email addresses to add his database. Not only do DHAs tie up mail resources, they compromise corporate directory information.

The 8300 Series includes detection and remediation against directory harvest attack. The following figure shows the overall flow. Note that this feature requires that administrators configure the appliance to synchronize with their LDAP servers that store user and group data to validate email address information for the organization.
To configure Directory Harvest Attack responses, administrators work with the spam settings section in the 8300 Series Control Center.

The screenshot above shows the default configuration. If, during a time window of 10 minutes, 80% of the recipients in a given sender’s messages don’t exist at the site, the 8300 Series will consider this a directory harvest attack. When that threshold is reached (both on a percentage basis on and on an absolute number basis) that sender is placed in a “penalty box” for a period of time, which, in this example, is 60 minutes. When a sender’s in the penalty box, the Email Firewall applies the action specified in the Action drop down list. Although there are other actions administrators can perform, the defer and reject actions occur at the SMTP connection-level. This a very efficient point to take action because it saves administrators from wasting mail server resources and accepting and processing messages unnecessarily.

Attack configuration is good to use in combination with the global approaches maintained by Symantec. It allows administrators to be as aggressive or conservative as administrators want to reduce mail volume from suspicious senders.

3.2.3 Global Reputation and Sender Group Management

In addition to local reputation analysis, the Email Firewall also analyzes global sender reputation by leveraging global sender data from the proprietary reputation services managed by Symantec. On an automated basis, Symantec’s Sender Reputation Service creates three separate lists that are automatically downloaded to customer’s sites:

- **Open Proxy List**—List of IP addresses with open proxy configurations or zombie vulnerabilities. Spammers typically use open proxy servers to send mail and evade detection. Previous virus outbreaks—Beagle for example—carried a payload that essentially converted millions of home user PCs into “zombies” machines that spammers could access to funnel spam and other email-based attacks. Thus, it’s quite dangerous to accept mail from an open proxy or zombie server. When implemented, this list blocks spam flowing through open proxies and zombies. If the 8300 Series is deployed at the gateway, the reputation check occurs on the connecting IP addresses. For post-gateway deployments, the 8300 Series can examine the SMTP headers and still perform reputation analysis.

- **Suspected Spammers List**—List of IP addresses from which virtually all of the outgoing email is spam (sent a minimum amount of email and has a very high percentage of that mail marked as spam by Symantec.) When implemented, this list allows mail from suspect IPs to be blocked.

- **Safe Senders List**—List of IP addresses from which virtually no outgoing email is spam (sent a large amount of mail for a considerable period without being marked as spam by Symantec). When implemented, this list allows legitimate mail to flow through to recipient immediately, bypassing further filtering.
Leveraging the data from the Symantec Sender Reputation Service, unwanted or abusive connection attempts can be handled on a site-wide basis based on the reputation of the sending IP address. Administrators configure automatic actions to global sender reputation matches in Sender Groups page of the overall Spam configuration.

While administrators can choose from a number of available actions, Symantec recommends connection level actions. Because connection-level actions occur before the Symantec Mail Security 8300 Series inbound MTA actually accepts the message, the net effect is a reduction in email volume that needs to be processed. For global sender reputation matches, administrators can choose from the following two connection-level actions such as:

- **SMTP Defer.** A temporary rejection, indicating to the sending email server to "try again later."
- **SMTP Reject.** A permanent rejection to the sending email server. In the deployment above, the configured action is to reject connections from Open Proxy Senders. This prevents the mail server from even accepting the connection and wasting resources.

Symantec’s approach to reputation filtering is multidimensional and quality-focused. As such, the Sender Reputation Service, along with the local analysis and action from SMTP traffic shaping feature, provides numerous advantages over traditional global sender databases. The benefits of the combined approach include:

- **Improved Global Sender data quality:** Symantec’s Sender Reputation Service obtains its Sender data from Symantec’s proprietary Probe Network and statistics from the protected anti-spam customer base, currently over 450 million mailboxes. The sender data is actively analyzed and the lists are regenerated on an hourly basis for maximum accuracy. Other global sender reputation databases simply aggregate data from dozens of third party DNS-based lists, which are often grassroots efforts that lack the active management and mitigation of false positives. In the case of Symantec’s Sender Reputation Service, customers never have to manage anything beyond specifying the action. Symantec manages the quality of the lists and dynamically rebuild them every hour to ensure accuracy.

- **No reliance on DNS lookups.** The Sender Reputation Service is distributed in a downloadable fashion, as opposed to relying on remote DNS lookups. Solutions that require DNS-based lookups to keep mail volumes to acceptable level will see their protection and performance collapse if DNS is unavailable.

- **Thwarts botnets and zombies.** The Achilles heel for global sender reputation databases comes in the form of distributed, low volume botnet or zombie-based attacks. Responsible for the majority of today’s spam, these attacks fly under the radar of global reputation systems, which are heavily volume-based. The 8300 Series, by maintaining a local reputation database, enabling administrators to quickly react to attacks at their particular site and block zombie or botnets attacks.
3.3 Spam protection powered by Brightmail

Accounting for over 80% of all email traffic, spam chokes the messaging infrastructure, saps mail server and storage resources, and clutters end-user inboxes. Offensive and fraudulent spam can create liability issues for organizations. Given the unbeatable economics and ineffective legislation, spammers will continue to flood organizations with unsolicited mail. As always, spammers will continue to adjust tactics and increase their volume to get around defenses that IT organizations deploy.

Multilayered anti-spam protection is the cornerstone of the Symantec Mail Security 8300 Series. Driven by technologies and response capabilities acquired from Brightmail, the filtering engine harnesses a robust arsenal for filtering techniques. These techniques include spam signatures, heuristics and machine learning, URL filtering, reputation-based filters, and other standard and proprietary approaches. The core filtering engine is designed to:

- **Catch 95% or more of spam.** Effectiveness—how much spam the solution can catch—is a key factor of any anti-spam solution. To maintain ongoing effectiveness, anti-spam solutions must constantly respond to the latest spam trends, categories, and dissemination tactics. Spam protection powered by Brightmail technology and response leverages over 20 different filtering techniques as well as a global spam analysis and response infrastructure. These elements help the Symantec Mail Security 8300 Series routinely deliver the best-in-class spam catch rate.

- **Ensure that legitimate mail is untouched.** False positives—the side effects of overaggressive anti-spam filtering—result in significant business problems, such as missing an important purchase order or missing an email from an important customer. When legitimate mail is being quarantined or otherwise affected as a part of the regular filtering process, that constitutes a failure. The Symantec Mail Security 8300 Series integrates the only anti-spam solution with a proven 99.9999% accuracy rate, which equates to less than one false positive in a million messages.

- **Maintain high performance.** An anti-spam solution that is performing poorly can cause mail queues to clog. In the best case, this leads to delays in e-mail arrivals and in the worst case can lead to a service interruption. Symantec’s filter creation workflow ensures optimal performance while maintaining high levels of effectiveness and accuracy. Manual, targeted filters spawn the automated creation of signatures, each of which addresses different spam characteristics. Filters are constantly weighted and tuned to minimize hardware performance overhead and to enable early termination of filtering. Among the tools and processes used to ensure that newly created filters are not causing a performance problem include performance test bed located in the Symantec Mail Security operation center as well as alert generation whenever a performance anomaly is noticed. If two alerts are recorded for the same set of filters, an escalation process is activated.

3.3.1 Spam scoring and configuration options

Unlike other anti-spam solutions that require frequent tuning and filter training to keep effectiveness and accuracy high, the anti-spam protection powered by Brightmail is entirely automatic. Every 5-10 minutes, updated filters and defenses flow from Symantec and are applied immediately on the appliances at the customer site. However, administrators can optionally adjust settings to customize anti-spam filtering at their site.

For example, administrators can choose to act more aggressively against “suspected spam.” When evaluating whether messages are spam, the spam engine calculates a spam score from 1 to 100 for each message. If an email scores in the range of 90 to 100 after being filtered, it is defined positively as spam. For more aggressive filtering, customers can optionally define a discrete range of scores from 25 to 89. To do so, the administrator just moves the suspect spam dial to the left (for example, to 80). As shown in the screenshot, messages scoring from 80 to 89 will be considered “suspected spam.”
Once a separate suspected spam score is configured, administrators can create a unique action for messages that are suspected spam. For example, they might choose a more conservative action, such as modifying the subject line and delivering it instead of deleting the message.

Another area of configuration is software acceleration, which allows administrators to run more complicated rule sets in memory for added effectiveness and performance. This technology does consume additional RAM, and is thus designed for 8300 Series appliances with 2GB or more of RAM.

### 3.3.2 Email Spam Quarantine

Email Spam Quarantine is an optional storage area for messages filtered by the Symantec Mail Security 8300. Using a standard Web browser, users can log in and review spam messages that the Symantec software has quarantined for them. Administrators can access the Email Spam Quarantine and configure settings from the Control Center.

The view above is an administrator’s view of the Email Spam Quarantine. That is, it shows messages that the 8300 series has quarantined for all users in their organization. If this was end-user quarantine, the Email Spam Quarantine view would only display messages addressed to that user. The overall look should be familiar to anyone who is familiar with web-based email. To search for a particular message, click Show Filters. To examine an individual message, click the subject. While browsing a message, additional options become available. If the message was incorrectly tagged as spam for example, the user can click Release to automatically send the message to the inbox and inform Symantec for analysis.

The Email Spam Quarantine can be an important part of a mail management policy. Organizations deploying Quarantine enjoy the following benefits:

- **Increased user confidence.** Viewing caught spam in a central quarantine shows end users the success of the filtering measures. Initially, end users prefer to see messages that have been filtered to assure themselves that no legitimate email is lost. As they become familiar with product’s accuracy, users will become confident that legitimate mail is rarely, if ever, quarantined. In the case of a false positive, or if users ever decide to keep a message, they can recover it with a few clicks.

- **Centralized and simple administration.** After initial customization, which includes specifying the retention period for messages and other settings, administrators don’t need to manage Quarantine. In the case of false positives, although administrators can review false positive submissions, there is no intervention required to get the necessary information to Symantec for incremental filter improvements.

- **Reduced loads on internal mail servers.** Downstream mail delivery, storage, and internal network traffic resources are decreased because quarantined spam is stopped before reaching the mail servers.

- **Automatic notification for users.** Although users can access their personal spam quarantine at any time, administrators can configure Quarantine to send an email summary at specific intervals. The summary lists the newly quarantined spam messages. Recipients of quarantine digest can click on secure hyperlinks to immediately release or view caught spam messages—without having to log in. This notification feature allows users to handle spam quickly and efficiently, rather than dealing with it on a daily or hourly basis.
Improved visibility into an organization's spam problem. Administrators have access to all quarantined messages and false positive submissions. The included search feature lets administrators perform quick queries and further examine the spam that is targeting the organization.

3.4 Email virus and outbreak protection

Viruses can wreak severe havoc in an organization. The damage ranges from email server crashes, system downtime, and the destruction of company data. From an email security perspective, the worlds of spam and viruses are intricately tied. About 80% of virus incidents are initiated by Internet-delivered email. In addition, the actual payload of many viruses and email-borne worms includes software that installs an open proxy on the target machine. These proxies are then used to turn the computer into a spam relay, which spammers then use to send even more spam. Given the damage resulting from viruses, it is essential to employ virus protection at the earliest point of network entry: the email gateway.

The Symantec Mail Security 8300 Series scans and detects viruses by integrating award-winning Symantec AntiVirus technology. Anti-virus protection includes automatic virus definition updates, flexible policies to handle messages with viruses, and specific defenses against mass-mailing worms and the associated spawned emails. The range of anti-virus features and technologies provide:

- **Real-time anti-virus content from Symantec Security Response.** The 8300 Series incorporates the award-winning anti-virus engine backed by Symantec Security Response. At Symantec Security Response, the industry’s largest team of experts works to identify and neutralize viruses before they can enter the network and spread across the enterprise.

- **Day zero virus prevention.** This feature leverages Symantec’s view of email threats as well as heuristic analysis to identify a suspicious attachment before AV signatures are available.

- **Proven protection against the latest threats.** Virus definitions are available every hour to ensure protection against the latest, fast spreading threats.

- **Rapid, reliable scanning and repair engine.** Actual scanning leverages the award-winning Symantec AntiVirus Scan Engine technologies. This award-winning engine provides rapid and reliable virus protection by scanning all incoming and outgoing Internet email traffic via a multi-threaded scanning system. It also repairs viruses within email attachments, including popular compressed file formats, such as zip, MIME/uu, TAR, GZIP, and others.

- **Maximum uptime during definition updates.** Unlike competitors, the modular Scan Engine updates virus definitions and scan engines without having to redeploy the software or restart services. Thus, there is no interruption in virus scanning to get new definitions.

- **Heuristics and variable scanning levels for more aggressive scanning.** The Symantec Mail Security 8300 Series uses Bloodhound™ heuristic technology, which detects virus-like behavior, to identify and repair unknown viruses. Administrators can adjust heuristic settings for more or less aggressive identification of viruses. The technology can detect up to 90% of new macro viruses and up to 80% of new and unknown executable file viruses, including malicious mobile code.

- **Protection against mail bombs.** Specify maximum size and scanning depth levels to reduce exposure to zip bombs that tax processing.

- **Multiple dispositions and actions.** Administrators can set up different policies to handle messages with dispositions, such as spyware/adware attachments, as well as unscannable. For example, administrators can clean and deliver, deliver normally, or delete the message.

- **Mass-Mailer Cleanup.** The virus protection features automatically remove not only the mass-mailing worm but also the associated spawned emails, which can number in the hundreds per recipient and serve no valuable purpose.
3.4.1 Day zero virus protection

The SMS appliance also delivers optional protection against day-zero viruses. While software vulnerabilities continue to be exploited faster and faster, it still takes a set amount of time to develop and roll out new virus definitions. The Suspect Virus module identifies nascent viruses and places them in a suspect virus quarantine while formal definitions are written.

In order to identify and delay suspicious attachments even before standard virus signatures are available, this feature leverages:

- **Probe Network analysis**: The technicians at the Email Security Group create suspicious attachment rules based on traffic analysis in the Probe Network. If the Probe Network shows this message/attachment appearing at an accelerating rate, or analysis of message shows suspect characteristics (file packing, misleading or obscured file type, similarity to known worm/viruses) then rules will be created accordingly and published to customers.

- **Heuristic checks**: These are rules and patterns published by the Email Security Group for messages that have generic characteristics of malicious content.

The following screenshot depicts the default policy for suspicious attachments, which is to remove the attachment and place the message in the suspect virus quarantine.

![Email Virus Policy](image)

The suspect virus quarantine, unlike the spam quarantine, is accessible only to administrators. The Suspect Virus Quarantine provides short-term storage of messages that are suspected to contain virus-infected attachments. Messages can be held for examination in the Suspect Virus Quarantine for up to 24 hours. The delayed messages will be released and rescanned in a configurable period of time. Administrators can also view, release, or delete delayed messages directly.

3.4.2 Signature-based Antivirus Configuration

Antivirus protection is a key component of the SMS appliance. Powered by the Symantec Antivirus Scan Engine technologies, the anti-virus engine identifies and cleans messages that contain viruses and related malicious executables. The scan engine incorporates updated signatures produced by Symantec Security Response to combat known virus as well as a heuristic engine to detect previously unknown strains.

In addition to determining if an attachment has a virus, the scanning engine can determine if the message is unscannable, encrypted, or carrying threats such as Spyware or adware. Administrators can leverage these different dispositions when creating overall virus policies. On a policy-basis, administrators can choose the action for each disposition. For example, an administrator might choose to clean infected attachments, but delete spyware attachments entirely.
Aside from creating virus-based policies, administrators also manage settings that control how virus scanning works at the site. For example, LiveUpdate is the process by which the system receives current virus definitions from Symantec Security Response. The following screenshot shows the available LiveUpdate configuration settings. By default, the appliance downloads certified virus definitions. To give administrators granular control over how anti-virus definitions are deployed in an environment, LiveUpdate provides the option of choosing newer, less tested Rapid Release definitions, or certified daily definitions.

Another powerful area of configuration is the Bloodhound level, which determines the way in which the system uses heuristics to flag viruses. Symantec Mail Security uses Symantec Bloodhound™ heuristics technology to scan for threats for which no known definitions exist. Bloodhound heuristics technology scans for unusual behaviors, such as self-replication, to target potentially infected message bodies and attachments. Bloodhound technology is capable of detecting upwards of 80 percent of new and unknown executable file threats. Bloodhound-Macro technology detects and repairs over 90 percent of new and unknown macro viruses. Bloodhound requires minimal overhead because it examines only message bodies and attachments that meet stringent prerequisites. In most cases, Bloodhound can determine in microseconds whether a message or attachment is likely to be infected. If it determines that a file is not likely to be infected, it moves to the next file. Lower heuristic levels may miss viruses, but consume less processing power, potentially speeding incoming mail processing. Higher heuristic levels may catch more viruses, but consume more processing power, potentially slowing incoming mail processing.

Administrators can also configure container settings and scanning settings that impact virus scanning. For example, when the 8300 Series processes certain zip files and other types of compressed files, these files can expand to the point where they deplete system memory. Such container files are often referred to as “zip bombs.” The 8300 Series can handle such situations by automatically sideling large attachments and cleaning them. There is a
presumption that such a file can be a zip bomb and should not be allowed to deplete system resources. The file is sidelined for cleaning only because of its size, not because of any indication that it contains a virus. Administrators can specify this size threshold and the maximum extraction level that the 8300 Series will process in memory, as well as a time limit for scanning containers. If the configured limits are reached, Symantec Mail Security will automatically perform the action designated for the “unscannable” category in the Policies settings.

### 3.5 IM Security

IM use in the enterprise has proliferated through grass roots adoption, devoid of the security considerations traditionally factored into the deployment of mission-critical enterprise communication tools. Symantec Mail Security 8300 Series directly addresses these concerns by providing a centralized solution for management, security, and policy enforcement for IM usage.

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature/Benefit</th>
</tr>
</thead>
</table>
| Threat Protection         | **Automatic Security Updates from the Symantec Mail Security Threat Center:** Receive automatic security updates for worms and spam lists from the Symantec Global Clearinghouse, part of Symantec Security Response.  
**Predictive Threat Protection:** Prevent zero-day attacks by using the Real-Time Threat Protection System (RTTPS) to detect malicious content using heuristic and behavior-based monitoring to recognize and block potential IM threat outbreaks.  
**File Transfer Control:** Choose to block or allow users from sending file transfers.  
**Virus Scanning for File Transfers:** Out-of-the-box integration with industry leading technologies from Symantec.  
**IM Client Version Control:** Prevent the usage of unauthorized versions of public IM clients that have not been patched or upgraded to address known security vulnerabilities. |
| Usage Control and Monitoring | **IM Screen Name Registration:** Require users to register their IM screen name with their corporate email address. Map real employee email addresses and attributes to their IM screen names.  
**IM Network Control:** Selectively disable access to specific public IM networks.  
**Identity Management & Screen Name Registration:** Provision IM user accounts, including support for single-user administration directly from the management console. |
| Visibility and reporting  | **Active user reporting**  
**Screen name visibility**  
**Spim reporting**  
**File transfer reporting** |
4.0 Content Filtering and Outbound Content Control

To conform to IT, regulatory, HR guidelines, organizations are increasingly looking to email security appliances to assist in managing policies for email. The 8300 Series includes new features to support a company’s regulatory and internal governance requirements. It also provides the tools to enable development of robust content compliance policies.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Policy management                     | • The ability to perform multiple actions and apply them to groups  
• Track multiple dispositions  
• Graphical condition builder  
• Pre-built policy templates, dictionaries, regular expressions for Regulatory Compliance and Internal Governance (requires Premium Content Control subscription)  
• Over 50 pre-built policy templates with references to over 100 pre-built Premium resources like dictionaries and regular expressions to enable a company to quickly build Content Compliance Filter Policies to classify email messages and address regulatory compliance, acceptable use and confidential data leakage. These templates and policies leverage content from Vontu, the leader in content monitoring and filtering market (requires Premium Content Control subscription) |
| Standard Detection capabilities       | • Scanning of all message parts  
• Extracts readable text from within attachments and containers  
• DBCS and High ASCII characters filtering  
• Attachment true file type detection. Instead of relying on the provided extension of an attachment, Mammoth determines the true file type of an attachment by analyzing its structure and signature. Supported file formats include .pdf, .zip, .tar, .doc., .xls, .ppt, and other 300 others  
• Seven pre-populated keyword dictionaries, including profanity, racial terms, sexual terms, and others. |
| Premium Detection                     | • Described content matching (dictionary and regular expressions)—Uses keywords, dictionaries, and regular expression pattern matching to detect data loss incidents or inappropriate content. Administrators can define or import a pre-defined dictionary of keywords or specify regular expression-based filters. Premium Content Control customers can leverage dozens of prebuilt managed dictionaries, including HIPAA, GLBA, CA 1386, VISA/PCI, OFAC, ITAR, and more.  
• Structured data matching using database extracts—Ensures detection accuracy for structured data, including database and tabular data such as customer, employee, patient or pricing data. Administrators can import a flat file extract of row/column data, define the data to protect on a field by field basis, set the minimum number of matched fields to constitute an incident, and specify combinations of fields that will not create an incident (exceptions). The upload process occurs using HTTPS and deployed index files are hashed with a 128-bit AES-compliant lossy encryption algorithm. Sensitive data is never stored in the clear. Structured data matching virtually eliminates the risk of false positives since the algorithm leverages an exact in-memory copy of protected database information. For example, an organization can monitor incidents of actual customer social security numbers and corresponding customer names leaving the organization as opposed to sorting through emails that contain content that happens to match a social security pattern. |
| Incident management and remediation workflow | • Policy-based incident generation Enables administrators to construct compliance policies such that messages matching a policy can trigger incidents, which can be tracked and managed.  
• Access-controlled incident folders Ensures that only appropriate reviewers can access messages that triggered incidents. Administrators or compliance officers can view messages that violate compliance policies, update the severity and status of the incident, and forward the message for escalation. Granular access control allows administrators give other users view only or modify access to specific |
folders.

- **Hold for review workflow.** Allows messages that trigger a content compliance policy to be temporarily held in a compliance folder, where the messages can be reviewed by a compliance officer. The compliance officer can then choose to accept or reject the message and automatically enforce configured actions.

- **Incident and compliance auditing.** Provides an exportable record of activity related to an incident, including when the incident was created, any subsequent actions, any changes in status or severity, along with any associated comments. The appliance also maintains a separate log of compliance related activity, providing visibility into which administrators changed a policy or compliance setting.

### Reporting

Provides a set of pre-built reports that present key metrics to quantify risk across the organization, inform management of regulatory liability, and demonstrate risk reduction over time. Administrators can generate higher level “dashboard” reports that summarize compliance trends across the entire environment or for a specific compliance folder.

### 4.1 Capability Walkthrough: Creating a Compliance Policy

Many organizations are under mandates to protect privacy and non-public personal information. For examples, several industry regulations, such as HIPAA and GLBA, have strict rules regarding the deliberate or inadvertent leakage of private customer data via email. In absence of such external mandates, most organizations store various types of customers’ private data, and this information must be protected in order to prevent loss of customer trust, brand damage, or identity theft. This section shows how the 8300 Series appliance can help an organization protect confidential customer data using pre-built Premium policy templates and supporting resources.

The first step in the policy creation process is to create a Compliance Incident Folder to store any incidents. Compliance policies can include a Create an Incident action which creates a copy of the original message that violated the policy in the Compliance Folder. Incidents can then be monitored and processed for appropriate action.

There are a number of configuration settings for compliance folders that administrators can leverage. In the screenshot above, a compliance folder named Customer Data Privacy has been created. As a policy action, an administrator can choose to automatically archive incidents. The Incident Management screens will leverage the text entering the archive tag field if the reviewer chooses the Archive action on an incident. The text entered in the archive tag field will also accompany the incident for easier searching and retrieval at a later date. Each compliance folder also has a notification template, and the administrator can also indicate if any users should be notified that an incident has occurred. Administrators can customize the format, content, and encoding for these notifications. Finally, when provisioning management accounts, administrators can assign access control for compliance folders, given view or modify access to specific folders.
Once the incident folder is provisioned, a data protection policy that leverages this folder can be created. When creating a new policy, administrators can choose from dozens of prebuilt policy templates that are populated to provide a quick route to implementation.

There are two types of data matching templates that can be created: structured data and described content. Structured data matching compares content in a message with records imported and securely stored into the system. Described content matching determines if message content matches a set of premium patterns or regular expressions. In general, because structured data matching works with a secure replica of exact data, it eliminates the false positive risk that exists with pattern-based or regular expression-based searching. An important consideration is that structured data matching does require access to actual customer data via database extracts. This may be impractical or impossible to obtain in some customer environments. The following table summarizes the key considerations to keep in mind when deciding on the detection technology to use.

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Described Content Matching</th>
<th>Structured Data Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td>False positive risk</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Scanning performance</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Access to access customer records</td>
<td>Not required</td>
<td>Required. As a safeguard, structured data indexes are only stored on disk in an encrypted hash format. The system uses a 128 bit AES-compliant algorithm.</td>
</tr>
</tbody>
</table>
In the policy configuration example shown below, a Described Content Matching policy has been selected.

A powerful aid to creating compliance policies is the Condition Builder. In the example shown here includes best practices tailored for the specific policy template. The conditions have built-in checks to reduce false positives. The Conditions box contains a number of compound conditions that have been defined to search for Social Security Numbers, Credit Card Numbers, and ABA Routing Numbers. These conditions reference Premium Dictionaries, Premium Patterns and regular expressions in combination to identify possible violations and eliminate false positives. For example, they use dictionaries that contain common words administrators might see in a message that contains a Social Security Number (since there may be numbers in messages that look like SSNs but are not).

The Actions drop down reflects that the administrator wants to temporarily hold messages that match incidents until a reviewer approves or rejects the message. When adding Hold message for review as an action, actions must also be assigned for when the message is approved or rejected.

Once the policy is saved, any incidents generated for the policy will be listed on the main incident management view for the folder, as show below.

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Message State</th>
<th>Severity</th>
<th>From</th>
<th>To</th>
<th>Subject</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Being Held</td>
<td>Unknown</td>
<td><a href="mailto:Mike.Smith@example.com">Mike.Smith@example.com</a></td>
<td><a href="mailto:sonora@domain.com">sonora@domain.com</a></td>
<td>Info</td>
<td>Jul 10, 2007 12:15:47 PM</td>
<td>New</td>
</tr>
</tbody>
</table>

Clicking on the message’s subject will enable a full view of the incident. Note that administrators can adjust the status and severity of compliance incidents and complete the approval or rejection of the incident.
5.0 Policy and System Management

For many email security products, the required administration effort makes the solution seem worse than the problem. Powered by automatic filter updates that require no intervention, Symantec Mail Security 8300 Series appliances can easily run in “hands-off mode.” The appliances are flexible enough, however, to accommodate administrators who want granular control of message filtering and policies.

5.1 Centralized Administration

The Symantec Mail Security 8300 Series features the Control Center, a Web-based interface that centralizes all administrative tasks. The following figure shows the overview page of the Control Center. This is the summary dashboard that an administrator will likely see when he or she first logs on in the Control Center.

Two key time-saving features of the Control Center administration model are:

- **Centralized and secure management.** Using the Control Center, administrators can view information on system status, administer the Quarantine, run reports, configure policies, manage users and groups, modify settings for all Scanners and other components, configure event-based alerts, and more—all from one intuitive interface. For added security, configurable access control lets administrators specify which computers or networks can access the Control Center.

- **Delegated administration.** To balance administration tasks, administrators can create additional administrator accounts, granting each administrator the desired level of management...
privileges for different components of the 8300 Series. For example, administrators might want to delegate management of Quarantine to another administrator, who will only be able to view and modify Quarantine settings. Alternatively, administrators can delegate incident folder review and actions to any individual who needs to review email policy incidents. Typically this would include compliance offices, HR, and legal employees.

5.2 Flexible Group-based Policies

Different groups or users in an organization may have unique filtering needs. Figure 8 shows an example of how different groups require very different handling of the same filtered mail. To precisely and easily map email requirements to different individuals and groups, administrators need a powerful and flexible mail policy management system.

5.2.1 Easy group definition

When creating different mail policies, a key step is to identify the user to whom the policy applies. The Symantec Mail Security 8300 Series makes it easy to specify who should receive specific policies. Administrators can create groups by:

- Synchronizing with a corporate directory. If an organization stores mailbox and distribution list information in an LDAP directory, the Symantec Mail Security 8300 Series can use pre-existing company LDAP groups to assign policies to group members. For example, to set up a policy for the sales team, Symantec Mail Security 8300 Series can query its local copy of the enterprise directory to determine the members of the sales group. This method reduces the ongoing administrative efforts to maintain separate lists. Because the Symantec Mail Security 8300 Series performs automatic LDAP synchronization, any updates administrators make to LDAP directories are automatically available. The LDAP-based features also include automatic distribution list and alias expansion.

- Manually specifying domains and email addresses. Administrators can also choose to specify users and groups based on email addresses or domain names (wildcards permitted). For efficiency, administrators can also import group members from a text file.

5.2.2 Multiple filtering dispositions and actions

The 8300 Series is able to precisely categorize filtered mail. This allows for unique policies based on the various categories of email. The Symantec Mail Security 8300 Series lets administrators choose from a host of actions, ranging from simply deleting the message, to performing markups and annotations, to actions performed at the SMTP connection level. For added control and flexibility, administrators can configure compound actions. For example, administrators might want to mark up a suspected spam message with text in the subject line and then send it to the Quarantine. The list of available actions is provided below.

- Add a configurable X-header to deliver it to the original recipient
- Add annotation or predefined text into the message (e.g., a legal disclaimer or custom footer)
- Archive, which delivers the original message and forwards a copy of the message to designated email address, and, optionally, a designated SMTP host.
- Blind-carbon copy (BCC) the message to the designated email address(es).
- Clean the message, which deletes or repairs virus infections. (Applies to anti-virus policies only)
- Create an incident (with hold for review option), which creates a record of a compliance or regulatory violation and moves a copy of the message (and attachment) to an optionally defined compliance folder. Optionally, the message can be held for review with the delivery deferred until an administrator or compliance officer has had an opportunity to review the message and approve or reject the actions.
- Defer the connection with a 4xx SMTP response code, tell the sending MTA to try again later.
- Delete message
- Deliver message normally, with no spam filtering or virus cleaning applied (logging still occurs)
- Deliver the message with TLS encryption, which routes the message using TLS encryption, using a specified encryption mode. This action help organizations comply with regulations such as HIPAA and GLBA, which mandate encryption of messages containing sensitive data.
- Forward the message to a designated address(es).
- Hold message in Spam Quarantine, which sends the message to the Web-based spam quarantine.
• Hold the message in the Suspect Virus Quarantine, which sends the message to a special delay queue for a configured time, after which the message is refiltered, using new virus definitions, if available. This action is only available for suspect virus dispositions.
• Modify the Subject line and deliver the message to the original recipient
• Quarantine the message to the Web-based Quarantine.
• Reject the connection using a 5xx SMTP response code, informing the sending MTA that the message is not accepted. Applies to connection management
• Remove invalid recipients. If a directory harvest attack is taking place, this action removes each invalid recipient rather than sending a message to the sender. (LDAP synchronization with a supported LDAP server is required).
• Route the message using the designated SMTP host.
• Send notification using a predefined notification text to the sender, recipient, or other designated SMTP address(es) with or without attaching the original message.
• Strip attachments, which removes attachment from message and sends message on to the recipient.
• Treat as [Allowed sender | Blocked sender] Processes the message using the action(s) specified in the domain-based Blocked Senders List or Allowed Senders List. This action applies even if the list is disabled, and applies to inbound messages only.
• Treat as [spam | suspected spam | virus | worm] Processes the message using the action(s) specified in the associated spam, virus, worm policy. The message is delivered normally if the associated policy is disabled or the policy doesn’t apply because of message direction.

5.3 Reporting
The Symantec Mail Security 8300 Series provides over 60 reports summarizing detailed statistics of inbound and outbound email filtering and IM security trends. The report data provides administrators with key metrics to show the value of the 8300 Series as a filtering solution at the site. Administrators can also leverage the collected statistics and trend information to help evaluate email filtering and policy compliance. The following figure shows an excerpt of a sample message overview report for email.

The reports provide the following features:
• Granular reporting. In addition to standard aggregate reports that provide a high level picture, administrators can drill down to all dimensions of email filtering. For example, administrators can see the effect of the SMTP traffic shaping by generating the Connections Management report. Administrators can also see which specific viruses have hit the organization, over email or IM. Many organizations would be interested to see which of the compliance policies have been firing. Armed with this information, administrators can take proactive measures, such as blocking specific domains and educating employees on how to avoid spam.
• Consolidated statistics in local time. The 8300 Series consolidates filtering performance for all Scanners deployed throughout the site without requiring additional licensing or configurations. Regardless of where the Scanners are deployed, reporting data is conveniently converted into the local time zone for display.
• Flexible generation and delivery. For convenience, administrators can configure the reports to be scheduled at configured intervals and emailed to recipients administrators specify. The scheduled reports can be generated automatically at configured intervals and administrators can decide the format of the report, including the export format. If administrators want to update management about the filtering metrics and the overall performance of the solution, administrators can add them to the recipient lists for appropriate reports. It’s a great way to show
results of the 8300 Series filtering at staff meetings. Administrators can also. Export report data for use in any reporting or spreadsheet software for further analysis.

5.4 End User Features

Administrators can optionally enable end users to manage and customize their filtering. Using LDAP-based authentication, users log into a special section of the Control Center and manage their personal spam quarantine and preferences that have been enabled by the administrator.

The customizable end user features include:

- Blocked Senders List—Users can specify addresses that will always be blocked. These entries supplement the organization-wide blocked senderlists defined by administrators.
- Allowed Senders List—Users can designate senders who are allowed to bypass anti-spam filtering.
- Language settings—Users can either specify languages in which they want to receive email or in which they don't want to receive email. Users can choose from 11 supported languages.
- Submissions—Users can submit false positives to Symantec for analysis.
- End-user Web-based Quarantine—Users on the network can log in to their personal quarantine at any time and view their quarantined messages.
- Quarantine message search—Users can search messages in Quarantine using multiple criteria, including To: headers, From: headers, message body, Subject: headers, Message ID: headers, and time range.

5.5 System Management Features

The 8300 Series has a full set of tools designed to make administration easy while still providing administrators the control administrators need.

- Flexible administrator rights—One time-saving feature is the ability to create flexible administration rights. Control Center administrators can be give read only or modify access to different tabs of the Control Center and to specific Compliance Folders.
- Message tracking—Administrators frequently need a quick and authoritative answer to the question, “What happened to the message I was expecting?” The 8300 Series Message tracking feature lets administrators or other users search for a given email message by subject, date/time range, envelope sender/recipient, disposition, next hop IP, and more. The Message Tracking feature provides an instant summary of the action performed on the message. For more detailed information, administrators can easily drill down to see a comprehensive, organized view of message’s flow through the system.
- Software update—Software updates provides an easy way to ensure that the appliance is always up-to-date from a software and security perspective. Whenever there’s an update available to the SMS appliance system software, the administrator will receive an alert. To perform the system update, all the administrator needs to do is choose the update, read the description, initiate the update, updates flow securely down to the appliance.
- Backup and restore—The backup feature lets administrators set up automatic or manual backups of all configuration and quarantine databases on the appliance at specified intervals. Administrators can store data on the local machine or a remote server. Then, using the Restore command, administrators can restore an appliance configuration from a previous backup.
- Automated alerts—Administrators can also set up automated email alerts. These alerts are sent to administrators or other parties when certain conditions arise. Administrators can specify what condition will trigger an alert on this page. Some examples include components not responding or working, anti-spam filters older than a specified time, or if the quarantine is low on disk space. Administrators can choose the types of alerts sent, the From: header shown in alerts, and the order in which administrators receive them.
- SNMP Support—In addition to the email-based alerts, the SMS appliance supports monitoring via Simple Network Management Protocol (SNMP) V2c. On the SNMP settings page, administrators can enable SNMP, specify the community string (similar to a password). If hardware events with the disk controllers occur, administrators can optionally provide a trap destination IP address that will receive traps. Aside from the traps, the SMS appliance supports passive monitoring of other hardware components, as well as MTA statistics.
- Logging—For logging information, administrators view information by component on a 7-point sliding scale. The settings can apply to individual appliances or to all. Administrators can also designate the maximum size and retention period for entries in the log database and save logs to a text file for further review. The SMS appliance also supports logging to a remote Syslog server.
- Troubleshooting Utilities—The appliance has a number of utilities that administrators can use to execute for troubleshooting or to determine status information about the system. The available tools include Traceroute, ping and others.
• **UPS monitoring**—The appliance supports monitoring of USB attached APC UPS devices and graceful shutdown upon loss of AC power

• **Command line access**—The SMS appliance has a set of commands administrators can use to configure, optimize and administer the system. Access these commands by logging into the system either through SSH or via the VGA or serial connections on the appliance.

### 6.0 Further Reading

This white paper provides just a glimpse of the feature set of the 8300 Series. It does not take the place of official product documentation or formal training curriculum that is available separately. For a comprehensive list of the features and benefits for the 8300 Series appliance, see the *Symantec Mail Security 8300 Series Feature Summary*. The *Symantec Mail Security 8300 Series Evaluation Guide Summary* provides a guided walkthrough of the Control Center, the powerful interface through which administrators manage policies and settings for the messaging gateway.