Symantec Brightmail™
Gateway v8.0
## Contents

1. **Executive Summary** ......................................................... 1

2. **Architecture Overview** .................................................. 2
   2.1 Flexible appliance deployment options .................................. 2
   2.2 Secure configuration .......................................................... 2
   2.3 Scanners and control center .............................................. 3
   2.4 Inbound and outbound email processing ............................... 4
   2.5 Public IM security proxy .................................................. 5
   2.6 Gateway-based deployment .............................................. 6

3. **Inbound Messaging Security** .......................................... 9
   3.1 The Foundation: Symantec response technologies and infrastructure ...................... 9
   3.2 Adaptive Reputation Management ....................................... 11
   3.3 Spam protection powered by Symantec Brightmail Antispam .......................... 15
   3.4 Email virus and outbreak protection .................................... 18

4. **Advanced Content Control and Data Loss Prevention** ............. 20
   4.1 Content Control Features .................................................. 20
   4.2 Capability walkthrough: creating a compliance policy .................. 22

5. **Policy and System Management** ...................................... 26
   5.1 Centralized administration ................................................ 26
   5.2 Flexible group-based policies ......................................... 27
   5.3 Reporting ....................................................................... 28
   5.4 End-user features ............................................................. 29
   5.5 System management features ............................................. 29

6. **Further Reading** ............................................................ 31
1. Executive Summary

Electronic messaging is a key enabling technology that can be leveraged to achieve business benefits. In today’s world of high volume, blended threats targeted towards messaging systems, securing a corporate messaging gateway has never been more challenging.

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

- Lost end-user productivity, wasted IT resources, and messaging infrastructure drain due to spam and unwanted email at the gateway
- Asset damage and downtime due to virus attacks and worm outbreaks
- Company brand or reputation damage due to phishing attacks or confidential data leaks through email
- The time spent by administrators deploying and managing messaging security solutions

At the same time, controlling the flow of information over email has become an increasingly important challenge. The stakes are high, as one in 400 emails contain confidential information. Companies need to control sensitive information, such as customer, employee, or patient data, as well as intellectual property in order to comply with internal and government regulations, fend off competition, and protect corporate brand and reputation.

The ongoing issue facing messaging administrators is how to preserve the value of messaging in light of escalating security threats and compliance requirements. Organizations are seeing an increased need for integrated secure content and threat management solutions that address multiple threats in a single solution.

The Symantec Brightmail™ Gateway (Brightmail Gateway) is Symantec’s award-winning response to the messaging security problem at the gateway. With Version 8.0—the latest system upgrade to the messaging security platform—organizations can:

- Stop spam, denial-of-service attacks, and other inbound email threats using industry-leading Brightmail Antispam™ technologies and response capabilities
- Leverage unique adaptive reputation management techniques that combine global and local sender reputation analysis to reduce email infrastructure costs by dropping up to 90% of spam at the connection level
- Filter email to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email
- Secure and protect other protocols, such as 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 Brightmail Gateway customers with an overview of the underlying architecture of this messaging gateway appliance and a walkthrough of the key capabilities of the product.
2. Architecture Overview
The power of the Brightmail Gateway begins with its flexible deployment options, gateway role, and ease of deployment.

2.1 Flexible appliance deployment options
Application specific appliances are becoming the platform of choice to secure the gateway. For maximum deployment flexibility, the Brightmail Gateway is available as a hardware or virtual appliance.

- **Hardware appliance.** As an all-in-one hardware appliance, the Brightmail Gateway integrates the core hardware and software pieces necessary for a comprehensive, secure, and easy-to-deploy messaging security solution. The Brightmail Gateway can be deployed on the Brightmail / Mail Security 8300 Series family of high-performance server appliances that scale across different deployment options ranging from small businesses to large enterprise customers. The appliances are rack mountable and include features such as redundant storage using RAID and dual power supplies and fans.

- **Virtual appliance.** For organizations that have adopted or are moving to a virtual environment, Brightmail Gateway Virtual Edition delivers all the benefits of the hardware appliance in addition to the benefits of virtualization. Such benefits include the cost savings due to better hardware utilization and lower power consumption, rapid deployment and provisioning, flexible storage options, and more robust backup and disaster recovery capabilities. Deploying the Virtual Edition on supported VMware virtualization platforms allows you to create a self-contained operating environment (a virtual machine) that behaves as if it were a separate appliance running the Brightmail Gateway. This allows you to deploy the latest Brightmail Gateway software onto the hardware platform of your choice. The Virtual Edition supports production deployments on VMware ESX Version 3.5 and VMware ESXi Version 3.5.

- **Mixed environments.** The Brightmail Gateway supports a combination of hardware and virtual environments. This allows customers to set up an infrastructure with physical appliances that perform mail scanning managed by a virtual Control Center appliance, which performs the centralized administration and hosts the spam quarantine, for example. Another popular application of this mode is to deploy a disaster recovery site running in VMware, while the production site leverages hardware appliances. Finally, in instances where you might require additional scanners during peak traffic times hardware based scanners can be supplemented with virtual based scanners for increased capacity.

2.2 Secure configuration
Regardless of deployment option, the Brightmail Gateway provides the same feature set in a secure configuration. A hardened, preinstalled Linux®-based operating system powers the Brightmail Gateway. The filtering and management platform software also resides on the appliance. In addition, there is an IM relay and embedded mail transfer agent (MTA) that enable email communication with both external sources and internal mail servers, such as Microsoft® Exchange and Lotus Domino. Software updates are easily applied, helping to ensure minimal disruptions for security updates.
To mitigate the risk of having email servers directly exposed to the Internet, Brightmail Gateway 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 MTA is secured against unauthorized relaying and buffer overrun vulnerabilities. Administration and management are protected by Web-based authentication, permitting access only by authorized users within the organization.

To ensure comprehensive protection against the latest email threats, the email security defenses are constantly fortified in real time with automatic antispam/antispim filters and antivirus definitions from Symantec, leveraging the global resources of Symantec Security Response and the Global Intelligence Network. 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 antivirus definitions are coming from Symantec. Filtering remains in effect while the appliance is receiving updated filters—so administrators remain fully protected, even during updates.

2.3 Scanners and control center
Each Brightmail Gateway 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 multiple appliances to perform specialized functions. The available functions are:

- **Dedicated Scanner.** Performs email filtering or optionally IM filtering. As a best practice, Symantec recommends provisioning separate Scanners for email and IM filtering. Administrators can set up one or more Scanner appliances. For load-balancing and high-availability purposes, multiple Scanner appliances can be configured using round-robin DNS and weighted MX records.

- **Dedicated Control Center.** Manages the Scanners at a site. Each Brightmail Gateway installation has exactly one Control Center appliance. The Control Center, which can manage multiple Scanner appliances, also hosts the email spam and suspicious attachment quarantines as well as storage areas for compliance incidents. The Control Center has been localized into English, French, Japanese, Traditional Chinese, Simplified Chinese, and Korean. The Control Center is responsible for functions such as centralized reporting, logging, policy management and message tracking. In the rare event that the Control Center goes offline, the crucial functions of message filtering and delivery continue uninterrupted 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.
2.4 Inbound and outbound email processing

When configured for email scanning, Brightmail Gateway appliances typically operate at the outermost gateway layer, responsible for processing incoming and outgoing email. For the core messaging platform, the Brightmail Gateway includes a powerful MTA, 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 pre-filtering checks based on the reputation of the source or IP connection, antispam filtering using Symantec Brightmail Antispam™ technology, award-winning Symantec Antivirus™ protection, content compliance and data loss prevention 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 and the global resources of Symantec Security Response and the Global Intelligence Network. Because Symantec performs all the filter updates, typical ongoing administration amounts to running reports to validate effectiveness and monitor mail flow. However, administrators who want more flexibility and control can use the suite of available management features. For example, they can choose to set up specific policies for email or IM messages identified as spam for different groups of users in an organization.

![Figure 1. Brightmail Gateway Architecture](image)

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 content compliance policies, such as Gramm-Leach-Bliley Act (GLBA) and acceptable use. First-generation solutions that 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 Brightmail Gateway 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, and 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, the Brightmail Gateway cleans the virus and holds the cleansed spam message in spam quarantine. This enhanced mail flow analysis feature accomplishes the key goals of reporting and acting upon multiple dispositions per recipient without performance penalties. The combined message analysis and conflict resolution occurs with no administrator intervention.

2.5 Public IM security proxy
In many organizations, IM use has proliferated through grass roots adoption, devoid of the security considerations traditionally factored into the deployment of mission-critical enterprise communications. The Brightmail Gateway directly addresses these concerns by providing a centralized solution for management, security, and policy enforcement for IM usage.

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.

When configured for optional instant message filtering, a Brightmail Gateway Scanner acts as a proxy for securing, managing, and logging multiple instant messaging protocols. A Brightmail Gateway appliance serving as an IM security proxy is typically installed behind one or more corporate firewalls.

The following table describes the features available when the Brightmail Gateway is configured to operate an public IM security proxy.
### Table 1. IM Security Features

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature/Benefit</th>
</tr>
</thead>
</table>
| **Threat protection** | • **Automatic security updates from the Symantec 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.  
• **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 and screen name registration:** Provision IM user accounts, including support for single-user administration directly from the management console.  
• **File transfer control:** Choose to block or allow users from sending file transfers.  
• **Extended feature control:** Enable or disable access to extended features such as audio/video conferencing, games, and file-sharing. |
| **Visibility and reporting** | • **Active user reporting:** You can view all active IM users that are currently signed on. With visibility to their IM account, email address, IM network, client version, status, IP, and the duration the user has been signed on.  
• **Screen name visibility:** Screen names from which the most IM messages have been sent. For each screen name, the report lists the total IM messages sent and the number of spam messages sent.  
• **Spam reporting:** The total number of IM messages, with the number and percentage of messages that were spam.  
• **File transfer reporting:** The total number of files transferred, with the number and percentage of files that contained a virus, were blocked, contained malware, or were encrypted. |

#### 2.6 Gateway-based deployment

From a deployment perspective, Brightmail Gateway 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 are behind the more restricted internal corporate firewall.

For larger installations, administrators can easily scale a Brightmail Gateway deployment by adding additional Scanner appliances that are managed by the single 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. This scenario can be further optimized for performance by modifying the roles for the Scanners. For example, administrators at each site can set aside one dedicated Scanner for inbound filtering and another for outbound filtering. Administrators can optionally dedicate a separate Scanner for IM filtering and control.

The diagrams that follow represent the most common and recommended deployment models for the Brightmail Gateway appliance.
This basic gateway deployment model is most suitable for smaller customers. The Brightmail Gateway is performing both the Scanner and Control Center functions. It resides at the outermost gateway layer, processing inbound and outbound mail, providing secure email services, and relaying mail to other relay layers or to the user-facing message store layer. With the appliance deployed at the immediate gateway, the appliance can minimize mail processing and storage requirements as well as network bandwidth via reputation filtering and connection management technologies.

Although similar to the basic gateway deployment, the multiple appliance gateway deployment model pictured above includes a dedicated Control Center used to administer multiple physical or virtual Scanner appliances that are responsible for email and IM scanning. The main benefit of this model is the ability to load balance traffic across multiple Scanners. Resiliency is also achieved as other Scanners can take over in the event of Scanner failure. This deployment model is suitable for larger customers with larger volumes of mail and where redundancy is a requirement.
Figure 4. Gateway Deployment - DMZ with SMTP Gateway

The above architecture shows the Brightmail Gateway in a multi-tier gateway deployment, with multiple Scanners in the DMZ and a Control Center behind a second firewall. This configuration has the same benefits as the multiple appliance gateway deployment and, in addition, meets a common security audit requirement: all data stores are in the second tier, including the Control Center, as it may store sensitive data. This approach may require more administrative overhead and complex networking than the other deployments.

Figure 5. Gateway Deployment with DNS Redirection for Public IM Filtering

The above architecture includes the relevant subset of a deployment when a Brightmail Scanner is configured for IM filtering. As depicted in the figure, the most efficient way to ensure that internal IM clients communicate with the IM security proxy in the Brightmail Gateway is by redirecting internal DNS. A typical transaction occurs as follows:
1. A user signs onto a public IM client with his or her 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 Brightmail Gateway Scanner rather than allowing the client to connect to the Internet and directly access the public relay.

3. The Scanner ascertains who the user is through screen name registration. The Brightmail Gateway 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 Scanner. 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 Brightmail Gateway Scanner.

This approach requires no client-side configuration changes or software installation and introduces no dependencies on inspecting specific ports that a client might circumvent.

3. Inbound Messaging Security

3.1 The Foundation: Symantec response technologies and infrastructure

An integral component of the Brightmail Gateway 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 as part of the Global Intelligence Network. These focused and coordinated operations centers, managed by Symantec Security Response, operate 24x7 and perform the following vital functions:

- **Real-time email threat monitoring with the Probe Network.** A key asset for the Symantec Global Intelligence Network 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.

- **Global reputation.** Using data collected from the Probe Network and Symantec's Global Intelligence network, Brightmail Operations tracks sender behavior to build a global reputation profile for IPs sending email. The reputation results are incorporated into the Symantec Global Bad Sender and Symantec Global Good Sender lists published by Brightmail IQ Services and made available to the Brightmail Gateway.
• **Virus definitions from Symantec Security Response.** To provide up-to-the-minute, round-the-clock protection, virus protection in the Brightmail Gateway is backed by Symantec Security Response. Here, 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 emerging threats.

• **Automated antispam filter creation.** Leveraging sophisticated tools, machine learning, and automated processes, Brightmail Operations creates defenses that eradicate current spam attacks and their variants. Using data from the Probe Network and statistics from the over 800 million mailboxes that Symantec protects, Symantec is able to create filters based on actual spam and monitor these filters to ensure very high accuracy rates. To combat emerging threats and new spam, Brightmail Operations also develops, tunes, and deploys other more proactive filters, such as heuristic-based filters. The Brightmail Gateway architecture represents a constant feedback loop, starting and ending with the customer site:
  1. At the customer site, the Scanner executes filters based on up-to-date protection from Brightmail Operations.
  2. Scanners constantly report back to Brightmail Operations regarding the effectiveness of deployed filters. If necessary, adjustments are made in real time by Brightmail Operations to improve effectiveness.
  3. Users at the customer site have the option to make missed spam submissions to Symantec.

• **IM Threat Center.** The Brightmail Gateway integrates with the Symantec IM Security Threat Center for automatic 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 automatic updates, the Brightmail Gateway frequently calls the Threat Center to pull the latest list of malware definitions, worm signatures, and spam signatures. Additionally, RTTPS receives high priority threat information from the global RTTPS community and the Threat Center. This threat information and worm signatures are automatically sent to the Brightmail Gateway to block any suspicious activity in the environment. Any malicious content signatures are analyzed by the Symantec Threat Center to validate the behavior and confirm that it is associated with a known or new outbreak.

• **Deployment of timely defenses.** Every few minutes, updated antispam filters and other email security defenses are pulled down over a secure connection to Scanners. 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 antispam filters.
3.2 Adaptive Reputation Management

Scanning email for spam, viruses, and compliance issues is a resource-intensive task. Any email that must be processed past the gateway taxes your mail infrastructure, resource capacity, and system performance. Stopping potential attacks is another reason to ensure that certain mail doesn't breach the gateway in the first place. A good example is the directory harvest attack, an abusive tactic that results in huge volumes of email and compromises an organization's email directory information. In these attacks, spammers send thousands of blank messages to mail servers in order to obtain legitimate email addresses. By keeping track of which addresses are not rejected, they can determine valid email addresses to be used in future spam or phishing campaigns.

The Brightmail Gateway features Brightmail Adaptive Reputation Management (Brightmail ARM). Brightmail ARM includes features designed to reduce unnecessary incoming email traffic, protect your network from attacks, and optimize the use of your processing resources.

Brightmail ARM includes technologies that can reject or defer incoming connection attempts based solely on the incoming IP address. To accomplish this, Brightmail ARM uses dynamic, self-learning local reputation data and connection classification to allocate system resources, global reputation data to reject malicious connections, and administrator-defined bad and good sender policies for customer specific requirements. Brightmail ARM leverages global reputation data based on the extensive world-wide data collection capabilities of the Global Intelligence Network, including Symantec's patented Probe Network. The Probe Network is Symantec's collection of millions of email accounts that collect spam throughout the Internet. The reputation results gathered from our networks are published by Brightmail IQ Services, Symantec's global reputation service. The Brightmail Gateway dynamically compares each sending IP attempting to send a message against Symantec's global reputation lists. Brightmail ARM additionally tracks local reputation data based on good and bad verdicts rendered by the Brightmail Gateway's content scanning analysis.

![Figure 6. Adaptive Reputation Management Flow](image)

The above figure shows a high level overview of how global and local reputation analysis is used with the Brightmail Gateway.
When a message is first received by the Brightmail Gateway, it is grouped into one of three top categories based on the sender's domain, IP, or address headers: bad senders, good senders, or mixed senders.

**Handling Bad Senders**

Bad Senders include IP addresses that are:

- Identified as a spam source from a global perspective by Symantec's Global Sender Reputation Service. The Symantec Global Bad Sender Reputation list is published by Brightmail IQ Services based on analysis of inputs from the Symantec Global Intelligence Network. With the 8.0 release, Symantec has expanded the number of IPs on this list by more than 10x over previous versions. Allowing the Brightmail Gateway to compare against a list in the tens of millions of IPs.
- Illegitimately sending mail. This category can include a broadband-connected PC that is infected by a botnet and is connecting directly to legitimate remote MTAs to send spam.
- Sending infected messages from an IP address. The Brightmail Gateway's email virus attack feature automatically detects such attacks.
- Launching a directory harvest attack. The Symantec Brightmail Gateway's Directory Harvest Attack prevention feature automatically detects such attacks by tracking a specified number and percentage of invalid recipients from an IP address.
- Identified on administrator-defined Bad Sender lists that are managed locally.

While administrators can choose from a number of available actions for dealing with Bad Senders, Symantec recommends connection-level actions. Because these actions occur before the Brightmail Gateway actually accepts the message, the net effect is a reduction in email volume that must be processed. For global sender reputation matches, administrators can choose from the following two connection-level actions:

- 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. This prevents the mail server from even accepting the connection and wasting resources.

**Handling Good Senders**

Good Senders include IP addresses that are:

- Identified as a legitimate sender from a global perspective by Symantec's Global Sender Reputation Service. The Symantec Global Good Sender Reputation list is published by Brightmail IQ Services based on analysis of inputs from the Symantec Global Intelligence Network.
- Identified on administrator-defined Good Sender lists that are managed locally.

Legitimate email messages take up the most resources to process. To help alleviate this resource consumption, the Brightmail Gateway can automatically track and verify local good senders. Messages from good senders can bypass all spam filtering, allowing these messages to be delivered with minimal latency while optimizing resource allocation.
To help manage this, the Brightmail Gateway includes Fastpass technology, which conserves resources by exempting senders with the best local reputation from spam scanning. The Brightmail Gateway automatically collects local sender reputation data to support Fastpass determinations and regularly re-evaluates senders granted a pass. Symantec Brightmail Gateway grants and revokes passes based solely on how many messages from each sender it determines to be spam. You can exclude specific senders from ever receiving a pass.

Handling mixed or unknown Senders
While acting on a sender's global reputation is an efficient way to identify and address high volume and known bad senders, it does have some limitations. For example, 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 focus on highvolume senders. Another category of senders who fall under the radar of global reputation approaches are those senders who are sending a mix of spam and legitimate traffic. In order to complete the picture for sender reputation, it is vital to also incorporate local reputation and factor in the mail traffic characteristics at the actual customer site. For such mixed senders, the ideal course of action is to not block them completely, but instead limit the amount of resources allocated to them and the impact of the resources they consume from the mail system.

Adaptive Reputation Management incorporates analysis and action on the local level with its Connection Classification feature. Connection Classification addresses botnet-driven spam and the unique complications inherent to mixed senders. Each Scanner tracks the reputation of sender IPs that are connecting to the customer site to determines whether they are malicious. Depending on how pervasive the malicious traffic is from a given sender, the Brightmail Gateway assigns incoming connections into one of ten connection class. Each class differentially allocates resources in order to limit the number of connections per IP or the number of messages per IP. At the bottom of the connection classes, the majority of connections are deferred. In conjunction with global reputation, this system can block up to 90% of spam at the connection level, while prioritizing resources for the delivery of legitimate email.

The following figure shows the dramatic up-front reduction in spam witnessed by a Symantec customer who leveraged the Connection Classification feature. In this case, over 50% of the unwanted connections were deferred by the Connection Class feature, which is in addition to the connections blocked by global reputation filtering.
One key benefit is the configuration simplicity. Instead of complex score management and threshold maintenance, the Brightmail Gateway ships with Connection Classification values pre-tuned based on best practices and Symantec’s experience. There is typically no need for customer intervention.

The Connection Classification features is a key requirement in resource optimization. Even in the face of spam attacks the Brightmail Gateway appropriately redirects resources to good senders so there is little to no latency in delivery their legitimate email.

Incorporating other actions at the local level
More often than not, email messages that arrive addressed to your domain but not to valid recipients are sent by spammers. When integrated with an LDAP directory, the Brightmail Gateway offers multiple methods for dealing with messages addressed to invalid recipients. This optional setting can be enabled in two ways:

- Reject at connection time. By using dynamic LDAP lookups to verify valid recipients, the Brightmail Gateway can reject messages to invalid recipients at the initial SMTP conversation with a 550 SMTP error.
- Silent delete. Messages to invalid recipients are silently dropped after acceptance, no bounce message is ever sent back to the sender.

Symantec recommends using the Invalid Recipient Validation feature in conjunction with the Directory Harvest Attack protection.
The Brightmail Gateway can also examine, detect, and mitigate possible directory harvest attacks (DHAs). 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 do not exist. This feedback from the server provides the spammer with the information he needs—valid email addresses to add to his database. Not only do DHAs tie up mail resources, they compromise corporate directory information.

The Brightmail Gateway includes detection and remediation against DHAs. Note that this feature requires that administrators integrate the appliance with their LDAP servers that store user and group data to validate email address information for the organization.

### 3.3 Spam protection powered by Symantec Brightmail Antispam

Multilayered spam protection is the cornerstone of the Brightmail Gateway. The Brightmail Antispam 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 more than 97 percent of spam.** Effectiveness—how much spam the solution can catch—is a key factor of any antispam solution. To maintain ongoing effectiveness, antispam solutions must constantly respond to the latest spam trends, categories, and dissemination tactics. Spam protection powered by Symantec Brightmail technology and response leverages more than 20 different filtering techniques as well as a global spam analysis and response infrastructure. These elements help the Brightmail Gateway routinely deliver the best-in-class spam catch rate.

- **See that legitimate mail is left untouched.** False positives—the side effects of overly aggressive antispam filtering—can lead to significant business problems, such as missing an important purchase order or an email from an important customer. Legitimate mail that is being quarantined or otherwise affected as a part of the regular filtering process constitutes a failure. The Brightmail Gateway has a proven 99.9999 percent accuracy rate, or less than one false positive in a million legitimate messages.

- **Maintain high performance.** An antispam solution that is performing poorly can cause mail queues to clog. In the best case, this leads to delays in email arrivals and, in the worst case, can lead to a service interruption. The Symantec filter creation workflow ensures optimal performance while maintaining high levels of effectiveness and accuracy. Manual, targeted filters initiate the automated creation of signatures, each of which addresses different spam characteristics. Filters are constantly weighted and tuned to minimize hardware performance overhead. Tools and processes are in place to keep newly created filters from causing performance problems, including a performance test bed located in the Symantec Brightmail BLOC and an alert generation system that is triggered whenever a performance anomaly is noticed. If two alerts are recorded for the same set of filters, an escalation process is activated.
Flexible Spam Scoring

Unlike other antispam solutions that require frequent tuning and filter training to keep effectiveness and accuracy high, Symantec Brightmail antispam protection is entirely automatic. Every few minutes, updated filters and defenses flow from Symantec and are applied immediately to the appliances at the customer site—or, administrators can optionally adjust settings to customize antispam filtering at their site.

For example, administrators can choose to act more aggressively against “suspected spam.” To determine 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.

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.

Bounce Attack Prevention

A bounce attack occurs when a spammer obfuscates message origins by using one email server to bounce spam to an address on another server. Spammers do this by inserting a target address into the "Mail From" value in the envelope of their messages then sending those messages to another address. If the initial recipient finds the message undeliverable, that mail server recognizes the forged "Mail From" value as the original sender, and returns or "bounces" the message to that target. When the targeted system recognizes the server from which the message was bounced as a legitimate sender, it accepts the message as a legitimate non-deliverable receipt (NDR) message.

Bounce attacks can be used to leverage the initial recipient's "good" reputation when sending spam, pollute the initial recipient's IP reputation, or create denial of service attacks at the target's server.

Symantec Brightmail Gateway uses bounce attack prevention to eliminate NDRs that are a result of such redirection while still delivering legitimate NDRs. To set up bounce attack prevention for your mail system, you simply specify a seed phrase and select the groups to which the bounce attack prevention will apply.

Once a system is configured for bounce attack prevention, the Brightmail Gateway calculates a unique tag based on a provided seed value as well as the current date. The scanner attaches this tag to outbound messages sent by users in defined groups. If the message is returned as undeliverable, the envelope's return address will contain this tag. By placing this tag on outbound messages and then checking inbound NDRs to ensure that the valid tag is present, the bounce attacks and "backscatter" will be blocked.

Email spam quarantine

Email spam quarantine is an optional storage area for messages filtered by the Brightmail Gateway. Using a standard Web browser, end users can log in and review spam messages that the Brightmail Gateway has quarantined for them. Administrators can access the email spam quarantine and configure settings from the Control Center.
The above picture is an administrator's view of the email spam quarantine. It shows messages that the Brightmail Gateway has quarantined for all users in the organization (or, for end-user quarantines, only quarantined messages addressed to a specific user). The overall look should be familiar to anyone who has used Web-based email. To search for a particular message, users click "show filters." To examine an individual message, users click the subject. Browsing a message makes additional options 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 an email management policy. Organizations deploying the quarantine enjoy the following benefits:

- **Increased user confidence.** Viewing captured spam in a central quarantine shows end users the success of the antispam filtering. Initially, end users often prefer to review messages that have been filtered for assurance that no legitimate email has been 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 should a user decide to keep a message—it can be recovered 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 the quarantine process. 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 quarantine at any time, administrators can configure the quarantine to send an email summary at specific intervals. The summary lists the newly quarantined spam messages. Recipients of quarantine digests can click on secure hyperlinks to immediately release or view caught spam messages—without even 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 extreme havoc in an organization. The damage ranges from email server crashes to system downtime and the destruction of company data. From an email security perspective, the challenges of spam and viruses are intricately tied. About 80 percent of virus incidents are initiated by email. In addition, the actual payload of many viruses and email-borne worms includes software that turns the target machine into a spam “zombie.” Spammers then access these zombies and use them to launch spam and other email-based attacks. Given the damage resulting from viruses, it is essential to employ virus protection at the earliest point of network entry: the email gateway.

The Brightmail Gateway scans and detects viruses by integrating award-winning Symantec Antivirus technology. Antivirus protection includes automatic virus definition updates, flexible policies to handle messages with viruses, and specific defenses against mass-mailing worms and the associated spawned email messages. The range of antivirus features and technologies provide:

• **Real-time antivirus content from Symantec Security Response.** The Brightmail Gateway incorporates the award-winning antivirus 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 the Symantec 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 protect against the latest, fast-spreading threats.

• **Rapid, reliable scanning and repair engine.** Actual scanning leverages the award-winning Symantec Antivirus scanning engine. This award-winning engine provides rapid and reliable virus protection by using a multi-threaded scanning system to scan all incoming and outgoing email traffic. It also attempts to repair 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 Symantec Antivirus scanning engine updates itself and virus definitions without having to redeploy the software or restart services. Thus virus scanning continues uninterrupted while new definitions are loaded.
- **Heuristics and variable scanning levels for more aggressive scanning.** The Brightmail Gateway uses Symantec 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 percent of new macro viruses and up to 80 percent 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 strain processing resources.

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

- **Mass-mailer cleanup.** Virus protection features automatically remove not only the mass-mailing worm but also the associated spawned email messages, which can number in the hundreds per recipient.

**Zero-day virus protection**

The Brightmail Gateway 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 Brightmail Operations, 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 can be created accordingly and published to customers.

- **Heuristics:** Brightmail Operations also generate rules and patterns to identify messages that have generic characteristics of malicious content.

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.
Signature-based antivirus configuration
Antivirus protection is a key component of the Brightmail Gateway. Powered by the Symantec Antivirus scanning engine, the antivirus engine identifies and cleans messages that contain viruses and related malicious executables. The scanning 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.

Automated virus updates
Aside from creating virus-based policies, administrators also manage settings that control how virus scanning works at the site. For example, the Symantec LiveUpdate™ process delivers new virus definitions from Symantec Security Response. By default, the appliance downloads certified virus definitions. LiveUpdate can also provide more frequent, less tested Rapid Release definitions, or alternatively the certified daily Platinum definitions.

Bloodhound technology
Another configurable setting is the Bloodhound level, which determines the way in which the Brightmail Gateway uses heuristics to flag viruses. Symantec Bloodhound heuristics technology scans 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. Lower heuristic levels may miss viruses, but they consume less processing power, potentially speeding processing of incoming mail. Higher heuristic levels may catch more viruses, but they consume more processing power, potentially slowing processing of incoming mail.

4. Advanced Content Control and Data Loss Prevention

4.1 Content Control Features
To conform to IT, regulatory, HR guidelines, organizations are increasingly looking to email security appliances to assist in managing policies for email. As summarized in the following table, the Brightmail Gateway includes several features to support a company’s regulatory and internal governance requirements as well as 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.  
• Over 50 pre-built policy templates with references to over 100 pre-built Premium resources, such as 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 loss. These templates and policies leverage content from Symantec Data Loss Prevention (formerly Vontu), the leader in content monitoring and filtering market. |
| **Advanced content filtering** | • 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 an attachment’s provided extension, determines the extension’s true file type by analyzing its structure and signature. Supported file formats include .pdf, .zip, .tar, .doc, .xls, .ppt, and 300 others.  
• Seven pre-populated keyword dictionaries, including profanity, racial terms, sexual terms, and others. |
| **Data Loss Prevention**       | • 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 predefined dictionary of keywords or specify regular expression-based filters. The data loss prevention capability can leverage dozens of prebuilt managed dictionaries, including HIPAA, GLBA, CA 1386, Visa/PCI, OFAC, ITAR, and more.  
• Structured data matching using database extracts—helps ensure detection accuracy for structured data, including database and tabular data such as customer, employee, patient, or pricing information. 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 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 any email containing 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 then be tracked and managed.  
• Access-controlled incident folders—makes sure that only appropriate reviewers have access to 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 to 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 they can be reviewed by a compliance officer. The compliance officer can then choose to accept or reject each message, triggering automatic enforcement of 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, and 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. |

Table 2. Brightmail Gateway Content Control Features
4.2 Capability walkthrough: creating a compliance policy

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

![Figure 9. Compliance Folder Configuration](image)

Administrators can leverage a number of configuration settings for compliance folders. In figure 18, a compliance folder named "customer data privacy" has been created. As a policy action, an administrator can choose to archive incidents automatically. 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 to facilitate search 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, giving "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, the administrator can choose from dozens of pre-built, pre-populated policy templates for a quick route to implementation.

Two types of data-matching templates 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 requires access to actual customer data through database extracts. In some customer environments, this data may be impractical or impossible to obtain. Table 3 summarizes the key considerations to keep in mind when deciding on the detection technology to use.
Table 3. Detection Technology Considerations

<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 customer records</td>
<td>Not required</td>
<td>Required</td>
</tr>
</tbody>
</table>

As a safeguard, structured data indexes are stored on disk only in an encrypted hash format. The system uses a 128-bit AES-compliant algorithm.
The condition builder is a powerful tool for creating compliance policies. 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 regulatory and data loss dictionaries, patterns and regular expressions in combination to identify possible violations and eliminate false positives. For example, they use dictionaries of common words that an administrator might see in a message containing a Social Security number (as there may be numbers in messages that look like SSNs but are not).

The "actions" drop-down allows the administrator to temporarily hold messages that match incidents until a reviewer has approved or rejected the message. When adding message held for review as an action, two actions must be assigned to the policy. The first takes effect if the incident is approved, the second if the incident is rejected.

Once the policy is saved, any incidents generated for it will be listed on the main incident management view for the folder, as shown in figure 12.

![Figure 12. Incident Management Folder](image)

Clicking on the message's subject will enable a full view of the incident. Note that the administrator can adjust the status and severity of compliance incidents and complete the approval or rejection of the incident, as shown in figure 13.

![Figure 13. Data Privacy Incident Management](image)
5. Policy and System Management

For many email security products, the required administration effort can make the solution seem worse than the problem. Powered by automatic filter updates that require no intervention, the Brightmail Gateway 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 Brightmail Gateway features the Control Center, a web-based interface that centralizes all administrative tasks. Figure 23 shows the Dashboard of the Control Center. This is the first screen an administrator will see upon logging in to the Control Center.

![Figure 14. Administrator Dashboard](image)

The Dashboard provides a dynamic view of system status and filtering activity for various timeframes. Administrators can use the Dashboard for at-a-glance metrics on the following:
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 various components of the Brightmail Gateway. For example, an administrator might want to delegate management of quarantine to another administrator, who will only be able to view and modify the quarantine and its settings, while delegating incident folder review and actions to any individual who needs to review email policy incidents. This would typically include compliance office, HR, and legal department employees.

### 5.2 Flexible group-based policies

Different groups or users in an organization may have different filtering needs. To precisely and easily map messaging requirements to different individuals and groups, administrators need a powerful and flexible mail policy management system. The Brightmail Gateway allows administrators to assign customized email and IM policies to specific user groups.

When creating different email and IM policies, a key step is to identify the user to whom the policy applies. The Brightmail Gateway 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 Brightmail Gateway can use pre-existing company LDAP groups to assign policies to group members. For example, to set up a policy for the sales team, the Brightmail Gateway can query its local copy of the enterprise directory to determine the members of the sales group. This method reduces the ongoing administrative effort required to maintain separate lists. Because the Brightmail Gateway performs automatic LDAP synchronization, any updates that 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.

The Brightmail Gateway is able to precisely categorize filtered mail, which allows for unique policies based on the various categories of email. The Brightmail Gateway lets administrators choose from a host of actions, ranging from simply deleting the message, to performing markups and annotations or performing actions at the SMTP connection level. For added control and flexibility, administrators can configure compound actions. They might, for example, want to mark up a suspected spam message with text in the subject line and then send it to the quarantine.

**5.3 Reporting**

The Brightmail Gateway provides more than 50 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 Brightmail Gateway 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. Figure 24 shows an example of the Reputation Summary report.

![Figure 15. Reputation Summary Report](image-url)
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 number of compliance violations occurring, the top compliance policies, and the incident outcomes by generating the Compliance Summary report. Administrators can also see which specific viruses have hit the organization over email or IM. 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 Brightmail Gateway 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 for display in the local time.

- **Flexible generation and delivery.** For convenience, administrators can configure reports to be generated automatically at scheduled intervals and emailed to specified recipients in html or pdf format. If management needs to be updated about the filtering metrics and the overall performance of the solution, administrators can add them to the recipient lists for appropriate reports. The Executive Summary is an ideal report to show results of the Brightmail Gateway filtering at staff meetings. Report data may also be exported for use in any reporting or spreadsheet software for further analysis.

### 5.4 End-user features

By integrating the Brightmail Gateway with the corporate LDAP server administrators have the option to enable end users to manage and customize their own filtering using the following end-user features:

- **Blocked senders list**—Users can specify addresses that will always be blocked. These entries supplement the organization-wide blocked sender lists defined by administrators.

- **Allowed senders list**—Users can designate senders who are allowed to bypass antispam filtering.

- **Language settings**—Users can specify languages in which they do or do not want to receive email, choosing from 11 supported languages.

- **Release**—Users have the ability to release false positives from quarantine; a sample of the message can be forwarded to Symantec and/or a local administrator 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 based on multiple criteria, including To: headers, From: headers, message body, Subject: headers, Message ID: headers, and time range.

### 5.5 System management features

The Brightmail Gateway has a full set of tools designed to make administration easy while still providing administrators the control they need:
• **Flexible administrator rights**—One time-saving feature is the ability to create flexible administration rights. Control Center administrators can be given read-only or modify-level 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 Brightmail Gateway message audit logging feature lets administrators 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. The administrator receives an alert whenever an update to the Brightmail Gateway software is available. To perform the system update, all the administrator must do is choose the update, read the description, and then initiate the update, which is securely distributed to the appliance.

• **Backup and restore**—Full backups or backups of specific subsets of the Control Center database can be scheduled to run automatically or may be run manually as one-time events. Administrators can schedule multiple backups to back up different database components at different specified intervals. Administrators can store data on the local machine or a remote server and then, using the restore command, restore the Control Center 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 and how often alerts will be sent. Examples of possible alert conditions include components that are not responding or working, antispam filters that are older than a specified date, and quarantines that are low on disk space. Administrators can choose the types of alerts that are sent, the From: header shown in the alerts, and which administrators will receive the alerts.

• **SNMP support**—In addition to email-based alerts, the Brightmail Gateway supports monitoring via Simple Network Management Protocol (SNMP) V2c. On the SNMP settings page, administrators can enable SNMP, specifying a community string (similar to a password). If hardware events occur with the disk controllers, administrators can optionally provide a trap destination IP address that will receive traps. Aside from the traps, the Brightmail Gateway supports passive monitoring of other hardware components, as well as MTA statistics.

• **Logging**—For logging information, data can be viewed by component on a 7-point sliding scale. The settings can be applied to individual appliances or to all. Administrators can designate a maximum size and retention period for entries in the log database and save logs to a text file for further review. The Brightmail Gateway also supports logging to a remote syslog server.

• **Troubleshooting utilities**—The appliance has several utilities that administrators can execute to troubleshoot a system or to determine its status information. 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 Brightmail Gateway has a set of commands administrators can use to configure, optimize, and administer the system. These commands are accessed by logging in to the system through either SSH or the VGA or serial connections on the appliance.

6. **Further Reading**
This white paper provides just a glimpse of the feature set of the Brightmail Gateway. For a comprehensive list of the features and benefits of the Brightmail Gateway appliance, see the Brightmail Gateway Feature Summary.
About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.