

SpamStopsHere Enterprise Edition

Greenview Data, Inc. developed SpamStopsHere, its anti-spam product and business with an intuitive control panel and specialized best of breed services based on the needs of the average customer and has done a great job at satisfying those needs. There is a great bit of flexibility in SpamStopsHere's standard package, and it's not a generic cookie cutter solution by any means. However, the fundamental design of our service and our anti-spam philosophy may not meet the needs of enterprise customers that have a user base or architecture that may demand something further. To address the needs of its customers, SpamStopsHere has strategically developed a product with the features most sought after by its enterprise users, called *SpamStopsHere Enterprise Edition*. If you are an organization, large or small, that needs any of the following features, then this product is for you:

END USER QUARANTINE

- Users easily sign up for quarantine service by visiting a URL provided by their administrator and typing in their email address
- Users can add additional email aliases to their quarantine service, making it easy to manage multiple email addresses with one login
- Users can view email quarantined as spam that was sent to their addresses in a fast loading format that can be sorted on any column (date, subject, from, to, filter that identified the message, etc.) and is sanitized of images and link tracking
- Users can delete messages, or with one click, have the message delivered instantly to their inbox
- Users can disable spam filtering for their email addresses
- Users can set up a daily report that is emailed to them that details the emails in their quarantine in an easily readable digest format in plain text, html, or in a spread sheet prepared CSV file
- Users can have a password reminder sent to them easily, without having to bother the administrator
- Administrator can perform maintenance, adding and deleting users from quarantine service

DOMAIN QUARANTINE

- Administrator has ability to view messages identified as spam and quarantined for all users at the domain in a fast loading format that can be sorted on any column (date, subject, from, to, filter that identified the message, etc.) and is sanitized of images and link tracking
- Administrator can delete messages, or with one click, have the message delivered instantly to the intended recipient's inbox

ADVANCED ATTACHMENT FILTERING

- In addition to having a message containing attachments with specific filenames or extensions removed from the email message and replaced with warning footer, you can have the email message itself be deleted or quarantined.

OUTGOING EMAIL FILTERING

- Monitor your network's security by using SpamStopsHere message submission service to send your outgoing email, filtering and alerting you on any spam or viruses leaving your network via email.

MULTIPLE CUSTOMER MAILSERVERS

- If you have your email server mirrored for backup or have multiple email gateways, you can have us relay your email to additional locations depending on availability and priority (much like private MX records).

EMAIL SERVER MONITORING

- Be notified by secondary email or by email to your cell phone if your email server becomes unavailable. Other alert options may become available as this is developed.

More detailed information is available on page 2.

QUARANTINE SERVICES

SpamStopsHere's philosophy has always been *not* to quarantine email. Other anti-spam products give a rating on how likely an email message is to be spam and still forces you to read your spam email and receive it in your inbox or in quarantine. Although it might be interesting to see that the heuristic anti-spam software has guessed correctly, when it does, it does not really save you any time. SpamStopsHere's approach was to use its industry leading accuracy to just *REJECT* the messages identified as spam. Because SpamStopsHere's proprietary URL/Phone# filter and Phrase filters are so accurate, it can actually save you the time of having to review the messages looking for false positives (messages incorrectly identified as spam). This ends up being an actual solution to the spam problem instead of just a neat gimmick. Additionally, if a message is incorrectly identified as spam, instead of the message sitting in a quarantine somewhere waiting to be read, the sender is notified right away that the message was not delivered, and can follow up if it is urgent. This can reduce the damage caused by an actual false positive, which are rare, but are the cause a greatest concern for most users of any anti-spam product.

However, many new users of the SpamStopsHere service may not believe the accuracy claims right away and will want to view all messages identified as spam for a while after signing up. Alternatively, your organization may have more than a few users who are skeptical because they have had horrible experiences with other anti-spam products. Therefore, although quarantine is against our philosophy, we have found that many organizations desire a method for this.

With the basic SpamStopsHere service, mail can be "quarantined" on an account wide level by selecting *FORWARD* as your action for a filter and forwarding the spam to a mailbox for review. This works well for small organizations, and is the default for the third party filters that users can subscribe to that are known to have a high false positive rate (Country Blocking and third party Real-Time Blacklists).

However, if you have a large organization, it can become daunting for the one person with access to the account where the spam is forwarded to go through all of the messages. As a result, we had typically recommended that large organizations just do not subscribe to these third party filters. Even small organizations should also unsubscribe from these third party filters if they do not wish to review spam for false positives.

However, the IT person of a large company, who is usually the point of contact for the SpamStopsHere service for their domain, will still be flooded with "missing email" questions from his or her users. Additionally, the more users you have, the more likely that you will have a small percentage of them that just do not trust the anti-spam service. As a result, end user quarantine service is important for larger organizations for scalability reasons.

The end user quarantine service will allow you to provide a URL to your users that they can visit to get started using the service. They will simply type in their email address, and a randomly generated password will be sent to their email address that they can use to access the quarantine for that account. The user is required to change their password the first time they log in, for security reasons. Once logged in, they can perform various actions.

These features make it so much easier for your IT person to determine where a "missing email" might be. You can determine if it actually was blocked as spam, or if it went missing somewhere else. Additionally, your users who are concerned about the anti-spam service can disable it for their entire account, or simply review the messages that are being identified as spam.

The Quarantine service acts as an additional filter option, so you can have it enabled for the filters you want. You can use it in addition to the regular filter options of *REJECT* or *DELETE*.

ADVANCED ATTACHMENT FILTERING

In addition to anti-virus service, SpamStopsHere offers Attachment Filtering. Many enterprise users who already have one or more levels of anti-virus protection may or may not want to subscribe to our anti-virus service for an added layer. On top of this, SpamStopsHere offers Attachment Filtering to all users. This filtering is based on the filename or file type extension of file attachments for email messages. The basic SpamStopsHere service allows you to remove all file attachments that meet a specific criteria, and have them replaced with a warning. This is useful for mitigating email based virus attacks by removing all attachment types that are executable (such as .exe, .com, .scr).

However, the enterprise user may have more advanced needs, and so features were added for them. In addition to replacing the file with a warning, *Enterprise Edition* users can select from our regular filter options and have the choice of *REJECT*, *FORWARD*, *DELETE*, and *QUARANTINE*. This allows much more control by your administrator, who may want to review what is being blocked or what is being sent to the domain under their control so that they can make changes or investigate any problems and enforce policy. Additionally, your organization might want to be able to block all zipped archive files (files ending in .zip), due to virus concerns but still be able to receive zipped archive files from clients where they can be forwarded somewhere to be retrieved by a trained administrator.

OUTGOING EMAIL FILTERING

In an effort to assist our customers with their security needs, SpamStopsHere is pleased to offer outgoing email filtering. With this service enabled, users' outgoing email will be scanned for viruses and spam by our industry leading filtering layers, before being seamlessly sent on to the recipient. Spam and viruses are removed, and the administrator notified, thereby helping to monitor and enforce your network's security policies. This security tool prevents spam and viruses from being sent from your network, thus protecting your network and clientele from virus proliferation and open relay concerns.

MULTIPLE CUSTOMER MAILSERVERS

The basic SpamStopsHere service already adds a lot of redundancy and reliability to your email system by assigning you multiple load balancers for your domain located in multiple data centers in multiple geographic areas of the U.S.A. and storing (or queuing) email for your domain should your email server become unavailable. For most clients that just have a single email server, signing up for our service increases the reliability of your Internet email exponentially. Some organizations also have a backup email server that will queue the email for their primary mail server if it should become available. This backup email server is completely replaced by the SpamStopsHere service, allowing you to appropriate the resources elsewhere, saving money.

However, some enterprise-sized businesses will actually have a backup or hot standby email server that is a live mirror of the primary one. Alternatively, your organization may have multiple email gateways (more than one public IP address for your email service, due to redundant Internet connectivity). In this case, you would typically want those delivering email for your domain to try the primary email server first, and then any additional ones, depending on availability. This is typically done with your domain's DNS MX records, but you lose this important function after signing up for our service, because you must point all of your MX records to us, and then you tell us what one place to relay your email to after it's been filtered for spam and viruses.

To address this issue, SpamStopsHere is developing a technology of internal private records similar to DNS MX records that will allow you to specify multiple locations to receive email for your domain, with priorities. The current work around is to update the location where we deliver your email, should the previous location become unavailable.

EMAIL SERVER MONITORING

Although most enterprise-sized businesses using our service will have monitoring in place and be notified within a few minutes of whether their email server is not functioning, adding another layer could prove useful. When subscribing to the SpamStopsHere service, you are adding another layer of service to your Internet email system. Why not have the ability to detect a problem between our service and yours? This service is being developed and will be configurable to send out alerts by email. You may have a secondary email address not at your domain where you can receive important alerts, or you can have the email delivered to your cellular phone for an instant page no matter where you are. Other delivery methods for the alerts may be developed.