



## PRODUCT EVALUATION GUIDE

**Anti-Spam Products**  
Insight's Technology  
Assessment Services (TAS)  
team has evaluated the  
following products:

- Symantec™ Brightmail AntiSpam
- SurfControl Email Filter
- McAfee® SpamKiller
- Trend Micro™ Spam Prevention Solution

### EVALUATING SPAM FILTERING SOLUTIONS

Unwanted solicitation via e-mail—otherwise known as spam—continues to be the bane of e-mail. Often considered to be the biggest nuisance on the Internet, the problem is shared by both enterprise and home users. Its elimination eludes legislators and IT managers alike; as long as the practice continues to be profitable, spammers will continue to flood e-mail in-boxes. But many products on the market now can greatly reduce the amount of unsolicited e-mail that makes it to your in-box.

Spam filters play an important business role for a number of reasons:

- **Productivity.** Employees no longer have to waste time deleting spam from their in-boxes.
- **Legal liability.** Much spam contains inappropriate and offensive material. An employee receiving this type of spam could potentially sue a company that allows its servers to receive it.
- **Network and server efficiency.** Reducing or eliminating spam at the gateway diminishes the amount of traffic on network and e-mail servers.

### KEY CONSIDERATIONS

#### Hardware requirements

Hardware requirements for spam filters vary depending on the type of solution you choose:

- **Hosted solutions:** Services that filter spam, viruses and any other e-mail-born attack by intercepting it before it gets to your network. Advantages: Few, if any, hardware requirements and a minimal administrative burden on your IT staff.
- **Appliances:** Stand-alone units with hardened operating systems, needing a PC only for accessing the management console. These solutions are gaining in popularity because of their ease of installation.
- **Server-based:** May require a beefy server platform to perform optimally, but possibly the least expensive option if you already have a server available. Before purchasing a server-based enterprise-class spam solution, confirm the hardware requirements as well as the operating systems it supports.

#### Administrative cost

The ongoing administrative cost of a spam filter varies depending on who is determining what is spam and what isn't. Some solutions put that responsibility into the hands of the e-mail administrator, while other solutions offer individual users control over what they define as spam. Some offer a Web-based portal users can log into, and some offer a Microsoft® Outlook client plug-in that lets users check their own junk mail folder. When the responsibility is given to users, e-mail administrators no longer have to police e-mail traffic.





### **E-mail system support**

Many spam filtering solutions on the market are agnostic, but it's a good idea to verify with the vendor that they support your particular e-mail solution.

### **Filter location**

Spam can be filtered at the gateway, the e-mail server or at the client. Filtering at the gateway means your e-mail servers won't be burdened by unsolicited e-mail, but small or medium-sized businesses with only one e-mail server may not have an SMTP gateway sitting in front of the e-mail server. They may find it more feasible to place the filter directly on the e-mail server.

### **Filtering methods**

There are several different methods used to filter spam. Real-time blacklists (RBLs)—databases of known spammers—are a popular method, but proving to be ineffective because spammers often use infected computers (zombies) to do the spamming for them. Other popular methods are white lists, heuristics, header analysis and image scanning. Bayesian filtering is extremely accurate, calculating a message's "spam probability" by learning from the user's selection of spam and non-spam. This method still works best at the desktop level. Another effective method is to algorithmically turn the e-mail message's body and header contents into a computer-readable number known as a one-way hash. This is then compared to a local or vendor-compiled database.

### **Benchmarking**

To accurately measure the effectiveness of your particular solution, you should keep careful records, noting the amount of spam you receive before implementation, during the tweaking process and afterwards.

### **Anti-virus integration**

Most solutions today have anti-virus integrated with anti-spam. If you happen to choose a stand-alone spam solution, check with the vendor to make sure it will integrate smoothly with your anti-virus solution.

### **Scalability**

Make sure the solution you purchase is the right size for your company, and that it will scale well as your organization grows.

### **Setup time**

Be clear on the resources required to configure your spam solution before you purchase it. Levels of sophistication vary; some solutions are pre-configured, providing basic filtering immediately upon installation. Others require training and manufacturer assistance.



### **Cost**

Most manufacturers price spam solutions based on the number of mailboxes to be filtered, so large-scale deployments can get expensive quickly. Make sure you have a good understanding of the manufacturer's pricing model before signing a contract.

### **Maintenance**

You may need to designate one or two full-time employees to administer an effective anti-spam solution, depending on the complexity of the solution, its ability to limit false positives and the size of your company.

### **Spam handling methods**

When e-mail is suspected of being spam, how will your filtering solution handle it? Most products give you the choice to reject it, quarantine it or tag it as spam before delivering it to the recipient. Until you get your solution properly configured, you should quarantine suspect e-mail, so you don't accidentally delete legitimate messages.

## **KEY FEATURES**

- **Anti-relay.** Prevent spammers from using your e-mail relay to send spam.
- **Report generation and customization.** Benchmark the results of your solution and establish a quantifiable return on your investment.
- **Inbound and outbound filtering.** Inbound filtering is basic to all solutions and may be all you require. But some solutions also filter outbound e-mail, as well as messages flowing internally between employees.
- **Customizable rule filters.** Most solutions provide basic filtering capabilities right out of the box, but you may find it necessary to customize rules to reduce the number of false positives. Some solutions have point-and-click rule creation, while others require Perl programming expertise.
- **Fail-over.** Depending on how critical you consider your anti-spam solution to be, you may want to be able to switch to a stand-by system in the event of failure.
- **Load-balancing.** High-volume environments may require load-balancing capabilities between anti-spam servers to provide optimal user throughput.
- **Cluster compatibility.** Large environments with clustered Microsoft® Exchange servers require a spam solution with this feature.



## CONCLUSION

Junk e-mail is here to stay, but your organization has a wide variety of options to choose from when confronting the spam problem. Insight has sales specialists ready to discuss your spam control needs, and a supporting staff of technical resources. We can be a valuable resource when you're trying to find the best solution for your particular situation.

**For more information, contact your account representative, or the Insight Technology Assessment Services team at [tas@insight.com](mailto:tas@insight.com).**

Insight and the Insight logo are registered trademarks of Insight Direct USA, Inc. All other trademarks, registered trademarks, photos, logos and illustrations are the property of their respective owners. ©2007, Insight® Direct USA, Inc. All rights reserved.



Insight®