

## OPINION: TECH DIRECTIONS

Jim Rapoza says the best way to stop unfair, confusing or simply outrageous pricing schemes is to just say no

PAGE 66



# Anti-spam challenge posed

LABS, SERVICE PROVIDER WISCNET TEAM UP TO EVALUATE SPAM-FIGHTING PRODUCTS, METHODS

By Debra Donston

**T**HERE ARE DOZENS, IF not hundreds, of anti-spam "solutions" available—be they stand-alone products

or applications integrated with other systems. So how do you filter this virtual spam of products to find the one that's right for your organization? That was the challenge posed to eWEEK Labs by service provider WiscNet, which is looking for a way to protect its customers from the growing problem of e-mail spam.

WiscNet—a non-profit, membership-based association of public and private organizations with primary emphasis on education, research and public service—provides services such as Web hosting, e-mail, Internet content filtering, Internet videoconferencing, commodity Internet and Internet2. The organization is developing new services to meet membership needs, including an anti-spam system. WiscNet's main

concern with spam, according to Technical Support Manager Kika Barr, is not so much the amount of bandwidth and resources that it

tem that can be used to hold these customers to their very different (and numerous) accountabilities.

Working with WiscNet,

30 responses. The final list of vendors and products tested during our eValuation was developed through a joint effort by eWEEK Labs and WiscNet's technical and management staff.

During the eVal, we wanted to evaluate anti-spam delivery methods as well as products. WiscNet was open to considering a hardware, software or service solution, so we chose two representative products in each of these categories.

It would be impossible to do a comparative test of every available anti-spam system. It would also be unnecessary—

most are more alike than they are different. The products we evaluated in this package were chosen for a number of reasons, including WiscNet's requirements, market leadership and eWEEK Labs'

[CONTINUED ON PAGE 62]



PHOTOS: eWEEK LABS



**Clockwise, from top left: WiscNet judges; eWEEK's Donston and Sturdevant; Sun Prairie Area School District's Loeffler; testing at the Pyle Center; CipherTrust's Mike Van Bruinisse.**

consumes at a backbone level but the effect it has on users and their resources.

WiscNet's constituencies include elementary, high-school and higher-education institutions; libraries; and government agencies. As such, WiscNet needs a very robust, flexible anti-spam sys-

eWEEK Labs Senior Analyst Cameron Sturdevant developed a detailed request for proposal that was sent out to a group of anti-spam vendors with at least stated ability to meet WiscNet's initial requirements. (The full RFP appears on Pages 64 and 65.) In all, we received about

Reviews of anti-spam software, hardware and services PAGE 58

# Six spam fighters face real-world test

**REVIEW:** WISCNET JUDGES RANK FLEXIBILITY AHEAD OF OTHER REQUIREMENTS

By Cameron Sturdevant

**A**FTER REVIEWING RFP responses from more than 30 anti-spam vendors, eWEEK Labs and service provider WiscNet invited six companies to show what they could do to help WiscNet solve its spam problem.

The results, following, are based on WiscNet's installation and initial use of each product in a variety of test environments that sought to simulate the vastly different constituencies that WiscNet serves. These include elementary-school, high-school and college students; faculty and administrators at all levels of education; and library staff.

In addition to comparing products side by side, we wanted to evaluate the different methods of implementation: software, hardware appliance and service.

We were surprised to find that the method of delivery is not as important as we thought it would be. For example, both Brightmail Inc.'s software system and FrontBridge Technologies Inc.'s service advocate a hands-off management approach. Likewise, both Postini Corp.'s service and ActiveState Corp.'s software products can be used out of the box without tuning but also let end users and administrators make changes to the way filters work based on specific user needs. Price will likely be the biggest differentiator in terms of platform choice. (Pricing for all the solutions we tested can be found in the chart on Page 61.)

Flexibility in administration was the No. 1 requirement for the WiscNet judges. Because it serves such varied members, WiscNet needs to be able to tune whatever solution it deploys in many different ways.

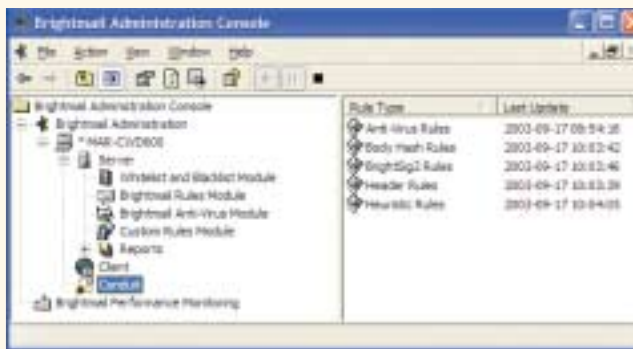
Judges representing the K-12 education constituencies, for example, said they would not want students to have access to quarantined e-mail, while judges from Wisconsin-area colleges said they need to be able to allow their professors a wide berth while granularly controlling access for students, administrative staff and many other groups.

WiscNet needs more flexibility than most organizations will, but there are few organizations that won't need to do some tuning and perhaps different tuning for different users. For example, an organization's executive-level managers may require access to filtered e-mail, while the clerical staff's filtered e-mail could be deleted without any quarantine at all.

However, generally speaking, we recommend that organizations put this kind of spam identification flexibility low on their list of anti-spam requirements. As the eWEEK eVal unfolded, we started to buy into the idea that spam is spam, and it should just be eradicated.

## ANTI-SPAM SOFTWARE ActiveState PureMessage

ACTIVESTATE'S PUREMESSAGE 4.0 takes a highly configurable approach to blocking



The dashboard view (top) in ActiveState's PureMessage server group manager helps administrators stay on top of spam and anti-virus statistics. Brightmail's administrative console (bottom) provides a modicum of control but always leans toward ensuring a low false-positive rate.

spam. The optional Domain Administration tool would allow WiscNet much of the end-user and domain administration flexibility it craves, but the additional price would also include up to 1 hour per week of administration to tune the filter rules.

Based on our work with WiscNet, eWEEK Labs recommends PureMessage for organizations that must allow users to opt out of anti-spam filtering and for organizations that want to filter more than e-mail that doesn't meet the official spam definition.

Of all the products we evaluated, PureMessage was by far the easiest to tune for par-

ticular mail characteristics. For example, its Policy Builder gave us nearly complete control over message handling rule creation. We could test for specific words and phrases and then define a wide range of actions to take on the message, from marking up the header to quarantining the message to deleting the message. The drawback to this much power is that mail administrators could easily change their spam problem into an anti-spam management problem.

Many judges perked up upon hearing about PureMessage's ability to check outbound e-mail for spam char-

[CONTINUED ON PAGE 60]

**REVIEW FROM PAGE 58**

characteristics. This could help organizations from inadvertently becoming the launch-point of a spam attack.

PureMessage uses many of the common techniques to effectively identify spam, including Realtime Blackhole Lists, malformed headers and pattern matching. Once messages are identified as spam, it is easy for users to check their quarantine folder. PureMessage can be configured to send an e-mail that contains a digest of all suspect e-mail. WiscNet and eWEEK Labs liked that users could resurrect messages from their own quarantine. The digest feature was easy to turn off (to prevent, for example, K-12 students from getting junk mail).

**Brightmail Anti-Spam Enterprise Edition**

BRIGHTMAIL ANTI-SPAM ENTERPRISE EDITION Version 5.0 is a high-profile spam blocker that uses a wide range of effective spam identification technologies, including proprietary blacklists, signatures and URL identification technology.

Like nearly all the vendors that answered our request for proposal, Brightmail claims to be 95 to 96 percent effective at blocking spam, and our experience at WiscNet seems to bear out that claim.

In fact, Brightmail borders on obsessive in its quest to maintain an extremely low level of false positives (legitimate e-mail that is mistakenly filtered). The company openly states that it would rather reduce the blocking rate than lose its claimed 1-in-a-million false-positive filter rate.

Brightmail uses a probe network that collects an undisclosed number of spam messages every day to constantly fine-tune the tools it uses to ferret out spam.

The platform uses six processing components, including signatures of spam messages, regular expressions and URLs embedded in spam that separate good mail from bad. The URL filter, which extracts the “call to action” URL address embedded in the mail message, was introduced this summer. Because the call to action is currently the hardest spam characteristic to hide, we think URL identification will put a serious dent in spamming efforts. We encourage IT managers to put this ability high on their anti-spam evaluation checklists.

Brightmail shoulders the burden of identifying spam based on its probe network. Because new rules and spam signatures are sent out securely from Brightmail to all customers every 10 minutes, we think IT managers will find the product effective at eliminating spam from user in-boxes.

The flip side of Brightmail’s management approach is that administrators lose a great deal of control, something the WiscNet judges were wary of.

Brightmail’s administrative control is likely more than sufficient for most organizations. Brightmail Anti-Spam allowed us to take the same action on all mail being filtered or to take different actions on two (and only two) domains. For example, K12.dane.wisc.



**Anti-spam capabilities are just part of IronMail’s e-mail security offering.**

edu could delete spam, while a.university.wisc.edu could place spam in quarantine.

**ANTI-SPAM HARDWARE  
CipherTrust IronMail**

BOTH OF THE HARDWARE-based appliances we evaluated included a lot more than just anti-spam capabilities because both come from companies with security roots that have grown into the anti-spam space.

IronMail grew out of CipherTrust’s work in providing firewall and intrusion detection for e-mail systems. The IronMail appliance is designed to withstand Internet-based attacks and is a good choice for organiza-

tions that are frequent targets of hack attempts.

In terms of its anti-spam capabilities, IronMail was among the most inflexible products we evaluated when it came to setting up different rules for different e-mail domains. This was a problem for WiscNet.

CipherTrust representatives indicated that a subsequent release of the product would allow administrators to apply rules by domain, but they could not provide a release date. While this lack of flexibility was a big weakness in WiscNet’s eyes, eWEEK Labs thinks that many corporations won’t miss the per-domain administration. When it comes to spam, most corporations likely feel the same as Robin Jarlsberg, technology director for the Cambridge, Wis., school district: “When it comes to spam, I just want it to be gone,” Jarlsberg said. “I don’t want end users digging around in a quarantine box.”

Mail administrators with a sweeping mandate to rid their organization of spam—and that should be a fair number—will likely be able to use IronMail as it stands today.

Aside from the usual anti-spam techniques that enabled IronMail to examine Wisc-



**SpamKiller provides only rudimentary information about its operation.**

Net's test traffic for spam characteristics—such as header and content analysis, including heuristics—IronMail also employs a statistical look-up service. Using information gathered from voluntary customer participation, e-mail messages are counted to see how often a particular e-mail has been seen by CipherTrust's clients.

In eWEEK Labs' experience, IronMail's statistical look-up service might prove to be more bluster than blockade because sophisticated spammers are rapidly figuring out how to modify messages to make them statistically different from one to the next. Even so, we advise IT managers to consider products as a whole. For example, Iron-

Mail uses myriad spam-stopping techniques, of which statistical look-up is just one that may add 3 or 4 percentage points of accuracy to the spam score IronMail assigns to incoming messages.

### McAfee SpamKiller

MCAfee SECURITY, A NETWORK Associates Inc. company, has

taken the open-source SpamAssassin and integrated it into its SpamKiller Anti-Spam gateway appliance. (The company acquired the famed open-source product in May 2002.)

SpamAssassin has had a long run as an open-source product and is still freely available at [www.](http://www.)

[CONTINUED ON PAGE 62]

## eVal score card: Anti-spam systems

| Product   | Pros  | Cons  | Cost*  | Overall recommendation   |
|---|---|---|--|--|
| <b>Software</b>   |   |   |  |  |
| <b>ActiveState's PureMessage 4.0</b>                                  | Usable out of the box, but almost all filter rules are fully configurable. Brainy support staff.  | Administrators who are tempted to make lots of filter adjustments may go from having a spam problem to an anti-spam management problem. It will likely be best to leave the controls in default until otherwise directed. | \$37,800 (software license based on number of processors, not per seat; estimate used five CPUs)         | PureMessage is a useful tool that shows a little elbow grease will provide organizations with a great deal of control over their anti-spam problem.  |
| <b>Brightmail's Brightmail Anti-Spam Enterprise Edition 5.0</b>       | Easy to install and maintain; administrators can take a set-it-and-forget-it attitude with this effective spam blocker. Backed by a massive research effort based on very high volumes of e-mail. | Users may want more control over what is filtered from their in-box. However, it's not clear that more control will reduce their spam or even the false-positive rate.  | \$92,450   | A benchmark in the field, Brightmail is a well-developed product that will likely overcome even the most obsessive e-mail users' concerns. The product is suitable for a wide range of organization sizes. |
| <b>Hardware</b>   |   |   |  |  |
| <b>CipherTrust's IronMail</b>   | Anti-spam and many other e-mail security capabilities in a convenient appliance form factor.  | Very little end-user customization capabilities.  | \$77,000 (licensed on throughput, not per seat; estimate assumes throughput of 150,000 messages per day) | The IronMail appliance has a lot of components to juggle and provides limited per-domain administration.   |
| <b>McAfee Security's SpamKiller Anti-Spam gateway appliance</b>       | SpamAssassin engine is a comprehensive spam blocker.  | Inflexible domain administration; requires administrator to resurrect false-positive messages. Rules are difficult to change and infrequently updated.  | \$51,295 (for one E1000 appliance)   | SpamKiller represents an unimpressive integration of the widely used SpamAssassin engine into a rudimentary anti-spam framework.   |
| <b>Services</b>   |   |   |  |  |
| <b>FrontBridge Technologies' TrueProtect Message Management Suite</b> | Blocked most spam; few false positives; secure, rigorously inspected data centers.  | Provides administrators with little control over what is classified as spam. Again, this is as much a pro as a con because the service effectively eliminates spam.   | \$1.15 per user per month, depending on services requested (\$207,000)                                   | For large enterprises that want to solve the spam problem with almost no administrative overhead, TrueProtect is a good choice.  |
| <b>Postini's Postini Perimeter Manager</b>                            | Very effective filtering; lots of user customization capabilities; has secure data centers, although fewer than FrontBridge.  | Not many. Administrators can dial down what options end users can change, making control freaks happy while dumping spam for the rest of the company.   | \$214,500 to \$300,000, based on volume and contract prepay  | Perimeter Manager is a good choice for effective spam blocking when end users also need control over how aggressively various filters sort mail.   |

\*5,000-seat scenario described in RFP (see Pages 64 and 65). Vendors provided published pricing for components based on eWEEK Labs' RFP. The figures make several assumptions, and we advise readers to take these numbers as a rough guideline only.

**EVAL** FROM PAGE 57

analysis of the RFP responses.

In preparation for an intense two-day evaluation, WiscNet also developed a list of eVal judges, including representatives from the constituencies WiscNet serves. (See next page for a complete list.) Prior to the eVal event itself, which was held Sept. 9-10 in Madison, Wis., technical staff from WiscNet worked with the anti-spam vendors to set up the applications.


It was during the program, held at the University of Wisconsin-Extension's Pyle Center, that the value of eWEEK's real-world eVal program really became evident.

Vendors' technical, marketing and sales representatives presented their products to the judging team. The judges grilled the vendors using their varied requirements: Can the product quarantine for some users but not for all? Wait, I don't want to quarantine at all—can you

just take the spam away? How granularly can I administer the product?

Organizations can judge by the way the products performed in this eVal how a particular anti-spam product and method will work for them. In its eVal format, eWEEK Labs has tested VPNs with the Defense Advanced Research Projects Agency, content management with USA Today publisher Gannett Co. Inc., mobile management with SBC Communications

Inc. and wireless LANs with Cornell University. WiscNet's Barr said, "This experience will help us make a well-informed decision on what to select for an anti-spam solution for WiscNet."

We will report WiscNet's final decision, as well as its experience with the chosen product over time, in a future issue. 

*Executive Editor Debra Donston can be reached at [debra\\_donston@ziffdavis.com](mailto:debra_donston@ziffdavis.com).*

**REVIEW** FROM PAGE 61

spamassassin.org. As such, SpamAssassin is a favorite test tool for spammers: A spammer develops a mail campaign, runs it against SpamAssassin until it gets through and, voilà, spam is waiting in your in-box.

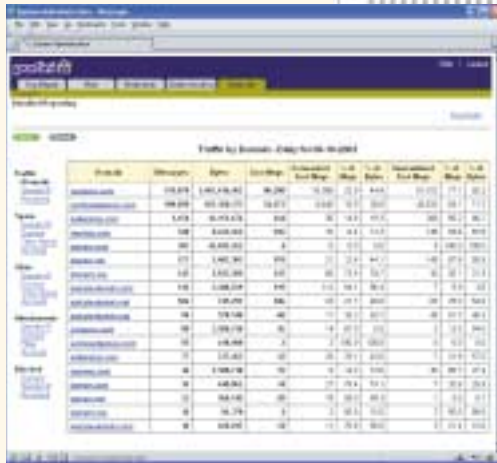
SpamKiller wasn't for WiscNet mainly because it requires that false positives be resurrected by an administrator. Company representatives said a forthcoming version of the product, due this quarter, will allow end users to resurrect filtered messages.

Probably the other biggest drawback to SpamKiller is that it is incapable of scanning HTML messages to determine if a message is spam. HTML is a favorite way for spammers to evade word- and character-scanning anti-spam devices such as SpamKiller.

Company representatives said SpamKiller in the future will allow for per-user policy creation but only for the forthcoming SpamKiller for Exchange (also due this quarter). eWEEK Labs thinks that an e-mail product that provides per-user policy only for the Microsoft mail

platform is too limited for consideration in most enterprises. We hope McAfee moves aggressively to develop policies for a variety of mail systems, including IBM's Lotus Software division's Lotus Domino.

With many of the other products we looked at, anti-spam updates were frequently released to



match the changing patterns and methods of the spammers. SpamKiller, in contrast, relies on 650 rules that are updated only on a monthly or bimonthly basis.

SpamKiller also doesn't lend itself to tuning by e-mail administrators. In fact, we



**The FrontBridge TrueProtect service (top) makes it easy for administrators to track spam and virus activity coming through the e-mail system. The Postini Perimeter Manager service (bottom) provides e-mail managers with detailed reports.**

were advised during the eVal not to adjust the characteristics of the rules because of the likely adverse effect on the filtering ability of the product.

These restrictions would be less troubling to us if it were not for the fact that most of the other techniques used by SpamKiller—techniques developed by McAfee before the acquisition of SpamAssassin—are fairly notori-

ous for providing false-positive results.

For example, as one of its five spam-testing components, SpamKiller integrates with third-party RBLs (Real-time Blackhole Lists), where suspected spammers are tagged by the Internet community at large. These lists are often managed by underfunded nonprofit organizations, and legitimate mailers sometimes linger on the RBLs.

**ANTI-SPAM SERVICES**  
**FrontBridge TrueProtect Message Management Suite**

ANTI-SPAM SERVICE

providers block spam before it even gets to an organization's mail servers, with no software or hardware to install or maintain. However, the service options are more expensive than the software and hardware options.

FrontBridge Technologies has a simple guiding principle when it comes to fighting spam: Spam has no place in the enterprise and should simply be done away with.

Even with this brassy atti-

tude, FrontBridge provides end users with two effective methods of checking their filtered mail for false positives: Users can either log on to a Web site for a list of messages, or an e-mail digest can be mailed to the user. In either case, the end user can be given the authority to resurrect false-positive e-mail. During tests at WiscNet, no false-positive e-mail was detected.

Although eWEEK Labs liked the FrontBridge approach, WiscNet wanted more per-domain administrative control than TrueProtect offers. In particular, WiscNet judges were leery of TrueProtect's limited white-list capabilities.

Aside from spam identification technologies, which we think are impressive and effective in TrueProtect, IT managers should consider privacy and security of e-mail when dealing with a third party.

We pressed company representatives on this point and feel comfortable recommending the company as a reliable, secure partner. FrontBridge data centers are

certified with the American Institute of Certified Public Accountants' SAS70 standards, which means that the infrastructure and data handling processes must pass rigorous third-party testing. The data centers are located throughout the United States, with additional locations outside the country. FrontBridge also implements extensive physical security procedures to ensure data privacy.

## Postini Perimeter Manager

THE POSTINI PERIMETER MANAGER anti-spam service requires that all MX (Mail Exchange) records for an organization's domain be directed to Postini's operations center. Thus, as with FrontBridge's TrueProtect, all mail is filtered before getting to an organization's e-mail servers and requires no hardware or software purchase.

Unlike TrueProtect, Postini Perimeter Manager does allow administrators to define spam management policies on a corporate, a group or an individ-

## Educate end users

Anti-spam products can filter out the most egregious spam e-mail, but end users should also be educated on how to avoid becoming a spam target in the first place. The following guidelines should be considered as a part of an acceptable-use policy:

- ▶ **Use your company e-mail address** for business use only.
- ▶ **Provide your e-mail address** only to trusted parties.
- ▶ **If you do need to make your e-mail address public**, describe it in a manner similar to the following: "ewweek at ziffdavis dot com."
- ▶ **Don't respond or attempt to unsubscribe to spam**; this serves only to validate your e-mail address. For the same reason, do not click on Web links embedded in suspect mail.
- ▶ **Report any spam** that you do get.
- ▶ **There currently is no officially recognized "do not spam" list**; signing up for a supposed do-not-spam list is likely equivalent to saying, "Yes, please send me even more unsolicited mail."

ual level. This pleased the WiscNet judges, but they had misgivings that e-mail would have to travel off WiscNet's network. WiscNet's desire to have all e-mail travel on its lines is a concern that most corporations do not share, and so we advise IT managers to put Postini high on their short list of anti-spam services.


Indeed, Postini Perimeter Manager's techniques for filtering spam were among the best we saw during the eVal. Where Postini differs is that Perimeter Manager caters to users' desire to twiddle with their spam settings.

Given the state of spam e-mail messages today—where nearly all are as obnoxious as they are unwanted—we can see the value in FrontBridge's flush-it-down-the-toilet attitude.

During tests, we could dial down racially insensitive mail to nearly zero but allow special offers through. (Hey, sometimes people really do want to look at mortgage offers.) We were also able to import lists of approved senders and block others, which is a nice feature for

consumers of special-interest newsletters that often look like spam to e-mail filters, including Postini's.

Perimeter Manager, like many other products in this review, scores e-mail messages after passing the message through several filtering engines to determine the likelihood that the message is spam. It became clear to eWEEK Labs and the WiscNet judges that this technique is an effective compromise that allows technology such as header and message analysis to catch the vast majority of spam without incurring a reputation for capturing good e-mail and sending it to the bad e-mail hopper.

We recommend that IT managers ask about the way anti-spam products protect against Internet-based mail attacks, including directory harvest attacks. Postini, for example, uses its Connection Manager feature to determine the characteristics of SMTP connections. 

Senior Analyst Cameron Sturdevant can be reached at [cameron\\_sturdevant@ziffdavis.com](mailto:cameron_sturdevant@ziffdavis.com).

## Anti-spam eVal judges

- ▶ **Shaun Abshere**, associate director, WiscNet
- ▶ **John Arechavala**, network and systems manager, Carroll College
- ▶ **Kika Barr**, technical support manager, WiscNet
- ▶ **Jane Dumke**, messaging manager, University of Wisconsin-Stevens Point
- ▶ **Robin Jarlsberg**, technology director, Cambridge School District
- ▶ **Pete Kretche**, network systems administrator, University of Wisconsin-Green Bay
- ▶ **Louis Loeffler**, supervisor of technology, Sun Prairie Area Public Schools
- ▶ **Paul Onufrak**, automation librarian, Eastern Shores Library System
- ▶ **Craig Stephenson**, enterprise services developer, WiscNet
- ▶ **Rich Turiel**, technical support specialist, WiscNet
- ▶ **Sheila Whitaker**, help desk analyst, computing and information technologies, Nicolet Area Technical College
- ▶ **Jim Young**, technical support, WiscNet

# Request for proposal: Anti-spam systems

Following is the request for proposal that eWEEK Labs sent out to vendors of anti-spam solutions. This document can be used as a starting point for your organization's own evaluation. This document can also be downloaded from <ftp://ftp.eweek.com/pub/eweek/antispamrfp.pdf>. (And if there's anything we missed, let us know at [eweek@ziffdavis.com](mailto:eweek@ziffdavis.com).)

Please respond to all questions and requirements. If the question or requirement does not apply, simply mark it "N/A." Your responses should follow the format of this document.

## Cover-page information

Company name \_\_\_\_\_

Complete product name, with version number \_\_\_\_\_

Release date (month and year) \_\_\_\_\_

Proposal authors \_\_\_\_\_

Date, company address and URL \_\_\_\_\_

Primary contacts with phone numbers and e-mail addresses \_\_\_\_\_

## Equipment list with version/model numbers and design description

An itemized list of equipment, if any, for each domain \_\_\_\_\_

An itemized list of software for each domain \_\_\_\_\_

An itemized list of services for each domain \_\_\_\_\_

A summary of your solution and what specific features it supports that put it ahead of the competition \_\_\_\_\_

## Price list of required products and services

An itemized price list of equipment for each domain \_\_\_\_\_

An itemized price list of software for each domain \_\_\_\_\_

An itemized price list of services for each domain \_\_\_\_\_

Summarize on one page the total cost of the entire project. \_\_\_\_\_

**Ongoing costs** Summarize the likely ongoing subscription and service costs needed to maintain the system over a period of three years. \_\_\_\_\_

\_\_\_\_\_  
 \_\_\_\_\_

**Product literature and documentation** Include product literature that describes the features and benefits of your equipment, software and services. Also include technical documentation for major components. \_\_\_\_\_

\_\_\_\_\_  
 \_\_\_\_\_

## Details

We understand that each customer is different and that these differences have a profound impact on equipment, services and cost of an implementation. Therefore, please provide as much context in your responses as possible.

Price, approximate cost per seat \_\_\_\_\_

**Price scenario 1:** 500 users, one office, 50 users work both in the office and on

the road **Price scenario 2:** 1,500 users distributed as: one main office in Madison (1,000 users), regional office in Appleton (250 users), regional office in Milwaukee (250 users); 300 users work both in an office and on the road **Price scenario 3:** 5,000 users distributed as: one main office in Madison (2,000 users), six regional offices (500 users in each regional office)

**Installation cost** One-time, nonrecurring expense to implement system

**Maintenance cost** Ongoing, recurring expense to operate system

**Training** Professional services, planning and design, consulting \_\_\_\_\_

## End-user experience

If spam rate was 40 percent of inbound e-mail prior to implementation, what is the expected percentage reduction in spam e-mail after implementation?

\_\_\_\_\_

## Quarantine

Describe quarantine review/message resurrection.

\_\_\_\_\_  
 \_\_\_\_\_

## Configuration

Can filter rules be manually changed based on new information? (For example: An incoming message is really spam, I mark it as such and the filter changes based on my manual action.)

\_\_\_\_\_  
 \_\_\_\_\_

## New screen artifacts

Tool bars, icons, system-tray icons

\_\_\_\_\_  
 \_\_\_\_\_

## In office vs. remote

Describe the end-user and administrative differences between your product used on the network vs. via remote access methods.

\_\_\_\_\_  
 \_\_\_\_\_

## E-mail evaluation

Describe the techniques and technologies that evaluate e-mail. (We expect this section to be substantial, without revealing trade secrets or other proprietary information.)

\_\_\_\_\_  
 \_\_\_\_\_

**Filters**

Filter process point: Where is the mail message handled?

---



---

Filter update

---

Filter customization per user

Filters developed from information provided by large numbers of users

---

Filters developed from honey pots

**Privacy**

Describe how information about an organization's spam is used to develop filters for other organizations.

---



---

What assurance does the end user have that e-mail contents will remain private?

---



---

What assurance does the organization have that e-mail contents will remain private?

---



---

What other concerns regarding privacy does your product address?

---



---

Where are quarantined messages stored? Describe what portion of the message is stored, if any.

---



---

Who reads messages?

---

**Reporting**

- |  |   |
|--|---|
| <input type="checkbox"/> Activity reports    | <input type="checkbox"/> Spam system change reports |
| <input type="checkbox"/> Database, if needed | <input type="checkbox"/> Integration                |
| <input type="checkbox"/> Mail platforms      | <input type="checkbox"/> Anti-virus                 |
| <input type="checkbox"/> User directory      | <input type="checkbox"/> Other products             |

**Operating platform**

- |                                  |                                  |                                |
|----------------------------------|----------------------------------|--------------------------------|
| <input type="checkbox"/> Windows | <input type="checkbox"/> Solaris | <input type="checkbox"/> AIX   |
| <input type="checkbox"/> HP-UX   | <input type="checkbox"/> Linux   | <input type="checkbox"/> Other |

**Security**

Describe how quarantined messages are secured.

---



---

Describe how report data is secured.

---



---

Describe how e-mail messages are secured as they are processed by the system.

---



---

How is access to the anti-spam solution protected?

---



---

Describe any other security-related issues that are associated with your anti-spam solution.

---



---

**User flexibility/scalability**

WiscNet serves a geographically dispersed client base. Further describe how your anti-spam solution can scale to serve thousands of users while maintaining centralized administrative support.

---



---

Describe how mail administrators can exercise local control.

---



---

Describe how users can control anti-spam filtering on an individual e-mail account.

---



---

**Administrative burden**

What skill set is required to be an expert administrator of your solution?

---

What skill set is required to be a front-line administrator of your solution?

---

When filters are updated, what action, if any, must be taken on the part of the organization?

---

During the next upgrade of your product, what product components, skill sets, product testing or other client activities do you anticipate?

---



---

**Language support**

What languages can your solution filter?

---



---

What languages does your solution support for the end user?

---

**Standards**

What standards does your product support?

---

What standards, if any, are in development that organizations should watch during the next year?

---

What legislation, if any, does your company support with regard to the curtailment of spam?

---



---