Rules for tools: Buying the right e-mail security product

By Joel Snyder

Buying e-mail security products is just like buying any security product -- sort of. While the same principles apply, the problem is that you have too many e-mail security choices. If you want to buy a database or an operating system, you basically have three or four options. Even for messaging systems, the field is pretty narrow. But start talking about antispam and antivirus technologies and you'll find dozens of products– each promising to be better than the next. That makes things more complicated and the decision-making process particularly difficult. Here's my advice.

Establish your requirements

I get a lot of e-mail from folks asking which of two antivirus or antispam products is better. These folks haven't done the first, and most critical, step in their search: defining requirements. When you know what you want a product to do, it makes the buying process simpler.

Most enterprises choose to "pre-treat" their e-mail before it hits their main messaging system (such as Exchange or Notes). So I'll use that as an example for how to pick products. Take a "divide and conquer" approach. Divide your search for e-mail security products into at least three components: antispam, antivirus and policy controls. Products that sit in front of the corporate messaging system usually have one or more of these components. Start by deciding what you require. If you're not sure, then stop right here – because you need to be sure. Whoever sent you on this wild goose chase must carefully define your company's needs.

Evaluate deployment options and performance

Let's continue by assuming that you want all three components. Next, see if your organization has any other global requirements, for example a preferred deployment model. E-mail security products are available as services, appliances or software you install on your own server. Is one strategy better for you than another? It's OK to say "no." You shouldn't make the deployment model a requirement just because it seems like a good idea.

If you haven't thought about outsourcing your e-mail security, now is the time to do so. You need to be sure whether a service-based approach benefits you before discounting it.

In the antispam and antivirus world, you'll **always** find a service component, either in the form of frequently automated updates or as a completely outsourced filtering system. Because antispam and antivirus are far from the core concerns of every enterprise, they are ideal technologies to outsource. Being "better" at antispam is not going to help your company manufacture safer widgets, I promise. So, it's not an area where you want to spend a lot of time getting good.

While you're considering these alternatives, think about performance requirements. You should buy a product or server that can accommodate your peaks (See sidebar on how to compute peaks). This is harder than it seems because many of the antispam vendors have taken an imaginative approach to describing their products' performance. For example, one up-and-coming appliance supplier quotes its performance as 10 times what it actually is, on the theory that 90% of your e-mail is spam and will get blocked. Don't fall for that kind of marketing sophistry. Test the products yourself or work with an independent lab to get true performance numbers for the products you're considering.

Determine if antivirus is a differentiator

You will need to refine your core requirements to narrow the field of contenders. Antivirus is a fairly stable market, so you're going to find it difficult to differentiate products based on their capabilities. One of the few factors that some vendors tout is "statistical antivirus," meaning they run each message through multiple scanners, any one of which can boot the message. Decide whether this matters and put it in your requirements if it does. Other antivirus techniques are available, such as heuristic antivirus and near-zero-day protection. If you consider antivirus a serious and primary threat, you may want to include these kinds of newer technologies in your requirement list.

Focus on users when choosing antispam

You'll find much greater variation in the antispam and policy-based controls of products, which makes it easier to disqualify products that don't meet your needs. For antispam, start with per-user capabilities. More than anything, this distinguishes products. Consider the following:

- Do you need a per-user quarantine?
- If so, how will users get to this quarantine?
- Do you want a Web-based system, an e-mail notification or both?
- How much control do you want to put in the hands of users?

You'll have several options for granting user control. Some products let end users create their own white and black lists. Others allow users to control spam sensitivity settings. Some take the tag-and-deliver approach, where e-mail is tagged with its "spam score" (typically in a header or the subject line), and filtering rules in the end-user e-mail client either file or delete the spam based on the tags. This gives the user instantaneous access

to their quarantine, at the cost of having to receive and store a great deal of unwanted e-mail.

If you're trying to minimize end-user interaction, make that a requirement. In that case, you don't want quarantine or per-user settings, and you certainly don't want tag-and-deliver. But you will need to be extraordinarily sensitive to false positives, so be sure you get greater control over various antispam settings. You might require the ability to tune pieces of the whole antispam engine or even to disable individual signatures. You definitely do **not** want to touch these things unless you absolutely have to, so don't require them unless you are serious about the need.

In any case, you need to decide on a strategy. I've looked at a lot of antispam products, and no single product excels at all strategies, no matter what the vendor claims. Choose your path ahead of time, and you'll be able to focus on the parts of the product that truly matter *to you* -- and avoid compromising on a product that does everything, but nothing very well. While many factors differentiate antispam products, user focus and control will do more to establish your baseline requirements than any other.

Review policy control carefully

Policy-based e-mail controls are integral to most antispam and antivirus solutions, but they vary enormously. Defining your specific needs will be critical to finding the right product. Policy controls usually end up as a combination of match rules and actions. Determine what kind of matching you need and the actions you require.
For example, if you want to look for keywords in documents your users are e-mailing out, get as specific as you can. Ask yourself:

- Are you going to search for a dictionary of words, account numbers or phrases? How big will the dictionary be?
- Do you need to look inside proprietary formats, such as a Microsoft Word doc or an Adobe PDF? If not, don't make it a requirement because it's an expensive feature.

If your policy control needs are simpler, say so. You don't want to pay for features that you aren't going to use.

Build a short list

Once you establish some basic requirements, use them to winnow the field of products. You don't have to go through a formal RFP process, yet. Share a few pages of notes and requirements with sales people to help them understand what you need and if their product is a good fit. No sales person wants to waste time talking to you if they can't meet your needs, and you don't want to waste your time studying the wrong products. Your goal is to come up with a short list of three to five products that all fit all of your requirements (at least on paper). If you have more than five, refine your list of requirements.

If you can't decide among the products you've short listed, then you have a good list. If you walk into the evaluation with a favorite, or (more commonly) thinking one product is not up-to-snuff, you're doing something wrong. If your short list is too long, consider other factors that will weigh on your final decision, such as pricing or the stability of the vendor. There's no point in looking at products you can't afford or that won't pass muster with your purchasing department.

From the short list, move into the lab. Products worth buying are worth testing and you want to put them through their paces. This is the time to get down and dirty with the features. For example, if you need footer stamping to add a disclaimer to outgoing messages, see if the feature actually works with real e-mail your company generates. If you're fighting spam, make sure that the product will work in your topology. It's not enough for a vendor to promise it works with Active Directory. The product has to be compatible with *your* Active Directory, and that's a lot easier to claim in a brochure than it is to make work.

Test the features -- *all* the features you're going to use. E-mail security is not a mature field, and many products still have substantial bugs in them. Configure the product and make sure that it fits into your company's architecture. If you don't get good vendor help now, you won't get good support later on. So this is an excellent time to evaluate the quality of the support team.

Haggle, haggle, haggle

Getting the best terms is an art in itself and beyond the scope of this column. Here's a quick hint, though: Don't start negotiations by admitting that the product is the one you want. Remember that everything is negotiable, and if the long-term support costs look high (and they usually do for this class of product), you have other pressure points you can bring to bear. They include training and professional services. Most of the e-mail security vendors are already giving away consulting services as part of the purchase, so be sure to get your share of free help.

About the author

Joel Snyder is a senior partner with Opus One, a consulting firm in Tucson, Ariz. He sent his first network e-mail in 1980, and has been designing and implementing enterprise e-mail systems ever since. He is partially to blame for the X.400 messaging standards and has been trying to atone for them ever since.

Sidebar: How to compute message peaks

To determine your peak per-second message load, take the number of messages you receive in a day and divide it by 10,000. Divide your total messages by 100,000 for the average load. For example, if you get one million messages a day, you are going to have

an average load of about 10 messages per second, and you'll see peaks of up to 100 messages per second.