

Software-as-a-Service a Good Choice for Fighting Spam

Neil Roiter, Senior Technology Editor
07.06.2009

It's tough to keep pace with the explosive growth of spam if you build an in-house email security solution. Commercial software and appliances are more efficient and have the features to make life easier for IT and end users, but even so, managing email security is just one more chore for companies with limited staff and tight budgets.

Small wonder Software-as-a-Service (SaaS) is increasingly popular among midmarket companies, and it's very likely a good choice for your organization.

The biggest consideration driving this trend is overtaxed staff. Even small companies have to deal with spam volumes that have grown far past the point where some basic filtering rules are sufficient. In-house anti-spam, using open source software such as SpamAssassin probably is no longer robust enough. What was initially a good, inexpensive solution put together and maintained by your technical hotshots, grows increasingly burdensome because either your hotshot is gone, or you're spending too much time keeping it up to date.

"After a while, running your operation and writing your own software and doing your own operational entity, you come to a point where technical talent is hard to keep," said Symantec director of product marketing Jack Musgrove. "You're not really running a formal IT shop; you're not keeping up with patches."

Shannon, Gracey, Ratliff & Miller, a Forth Worth, Texas-based law firm, is typical. IT director Amy Olson and her network admin comprise a staff of two supporting 150 employees, including some 70 attorneys in the main office and five small branches in the state. They maintained a Linux-based SpamAssassin server.

"We had to constantly do updates. It was just another server that needed care and feeding," she said. "On top of that, we'd have to manually manage requests to block this person or allow that person. It was taking up a lot of our time on a daily basis."

Olson said 80% or more of the firm's email was obvious spam, putting a lot of unnecessary strain on her networks and taking up disk space that needed clearing.

A SaaS alternative made all that go away for her shop. Olson switched over to Postini's email security services about 16 months ago, shortly before the service provider was acquired by Google. For something more than \$2 per mailbox, she and her network admin are free to focus

on projects that have real business value instead of answering help desk calls and treading water to keep from being overwhelmed by spam. And while email appliances are a very viable alternative, they still require some care and feeding. Most small IT departments have better things to do.

"They don't want to have to go through fine-tuning and tweaking filters," said Forrester analyst Jonathan Penn. They don't have the skill set and they don't want to have skill set. They'd rather spend the money hiring someone who's savvy in something else that has a lot more relevance."

Cooling and high availability factors to consider

Olson notes that an email appliance is "just another thing that requires cooling; you have to have a UPS, and you have to monitor and manage it."

High availability is another consideration. Email appliances are very reliable and unlikely to go down, but it's a consideration. If you can't afford an outage, you'll need to run a second appliance in parallel in case one goes down. That's not a very attractive option for small organizations because of the extra cost and maintenance. On the plus side, vendors typically offer deep discounts for backup appliances.

On the other hand, SaaS vendors are well established with strong, redundant infrastructures, and SLAs that guarantee availability.

"You're buying an insurance policy for uptime," Musgrove said.

That appeals to Olson, who considers an email appliance "another point of failure on my network." She said that when Google had an outage, service continued transparently. The only impact was that reports weren't available for a while.

Weighing appliances versus services

If you go the SaaS route, you're treating email security as an expense rather than a capital expenditure. If that's your preference, one of the prime advantages is that you pay as you go for the number of users. So, if your company has laid off employees in this tough economy, you can ratchet down and increase your costs as your employee count goes up. That may be more attractive to management than additional capital investment.

On the other hand, if data leak prevention is a major consideration, an appliance may be a better choice, and may be important enough to outweigh the powerful arguments in favor of SaaS. Your company may insist on controlling outbound email content in-house and implement DLP and email encryption internally.

Archiving and e-discovery are also considerations. Most service and appliance vendors also offer these services, which are increasingly important because of regulatory requirements. Some companies are reluctant to turn the sensitive information in emails over to a third party for storage and retrieval, but smaller companies -- and some enterprises as well -- generally don't want the expense of buying, integrating and managing archive infrastructure.



Shannon, Gracey, Ratliff & Miller is a prime example. Even with the sharp reduction in spam, email volume has increased tremendously, both in numbers and attachment size. So, they've recently started phasing in archiving and e-discovery service.

"Even we thought we stopped the spam issue, our information store was growing larger and larger and larger," Olson said. "We needed something to set retention policy, and our attorneys wanted to be able to access several years back, [and we] wanted to do that without latency."

One caveat: Be prepared to pay a one-time fee to migrate your in-house archive to the service or appliances. Even a small firm like Shannon, Gracey, Ratliff & Miller had 3.5 million messages that had to be exported.

SaaS vs. on-premise options

If you are unhappy with your current vendor, or your current contract is coming up for renewal, it's time to consider your options. Both SaaS and on-premise products will provide efficient anti-spam and good email antivirus.

One route is to go through your network service provider. Your traffic is already going through them, and most offer email security services. If you're comfortable going with whatever vendor they work with, it's a painless way to offload email security.

Price of an appliance versus a service may not be the major differentiator it once was. Hardware vendors are offering attractive subscription models and deep hardware discounts to get their product through your doors. So consider the other factors we've discussed and see what kind of prices you can negotiate.

Nonetheless, the SaaS model is looking pretty irresistible for most smaller companies.

"Really a no-brainer to go into direction of service providers," said Forrester's Penn. "There's really no good reason these days for a smaller organization that doesn't have that kind of expertise in-house already, that kind of staffing, that kind of competency dedicated to email management to go with a product."

