

Hybrid E-mail Security: Integrating SaaS and On-Premise Solutions

By **JEFF WILSON**
Principal Analyst, Security
Infonetics Research, Inc.

JUNE 2010

HYBRID E-MAIL SECURITY

E-mail-borne threats and spam are ubiquitous problems with no end in sight. No company can afford to be without an e-mail security solution, and most companies around the globe have made some level of investment in e-mail security, but there are still threats and victims.

If a company has invested in an e-mail security solution and still finds it has an insurmountable spam problem, or still finds its employees falling victim to e-mail-borne threats, it often has to do with the way e-mail security is purchased and rolled out. **For many companies, e-mail security purchases are reactive.** Everything is clicking along perfectly one day, and then the next day there's simply too much spam to effectively deal with, and mail servers slow down to a crawl. This is followed by the inevitable IT fire drill and the purchase of a product that may not solve the long-term problem.

Purchasing e-mail security solutions this way often leads organisations to have mixed environments, with e-mail server gateway and hosted solutions layered in the same network. There are many hosted/SaaS e-mail security solutions available, which solve some deployment problems and help IT departments come to terms with massive volumes of spam and e-mail-borne threats. However, they add an additional layer of management complexity because they are generally deployed on top of existing on-premise gateway hardware or software security solutions.

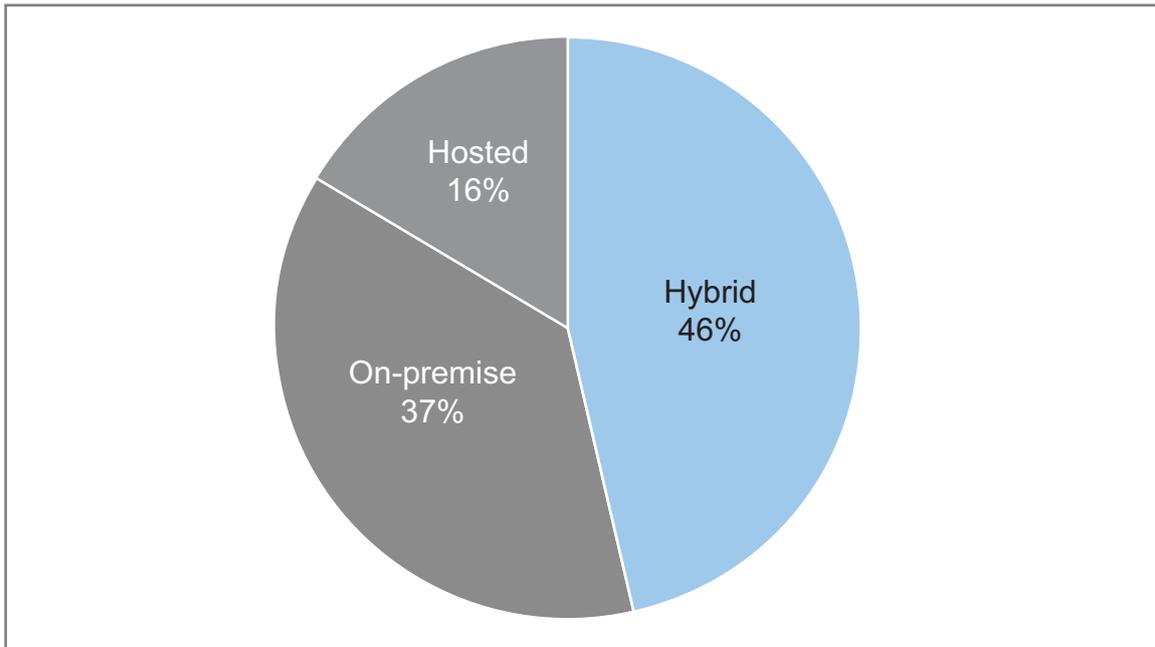
We suspected that there are many organisations using hybrid e-mail security solutions created by deploying hosted/SaaS security in addition to their existing on-premise e-mail security products, often from multiple vendors. We lacked the proof however, so we devised a survey to find out how common this practice really is, what issues customers are trying to solve with these hybrid solutions, and respondent interest in an integrated hybrid e-mail security solution from a single vendor.

Using a panel of qualified IT decision-makers, in May 2010 we conducted a web survey of 150 US organisations that have at least 1,000 users in their e-mail environments. Survey respondents have detailed knowledge of the e-mail security products and services their company uses, and have influence in the e-mail security purchase process. This paper discusses the results of the survey and our conclusions based on those results.

IT'S A GRASS-ROOTS MOVEMENT

First we asked respondents what types of e-mail security solutions they have deployed. Thirty-seven percent use on-premise solutions only (software or appliance gateway products), while 16% use hosted solutions or SaaS only. The single most significant finding of this survey is simply this: **nearly half of respondents, a random sample of enterprise e-mail environments, have a "do-it-yourself" hybrid on-premise and hosted solution.**

USE OF HYBRID E-MAIL SECURITY IS WIDESPREAD

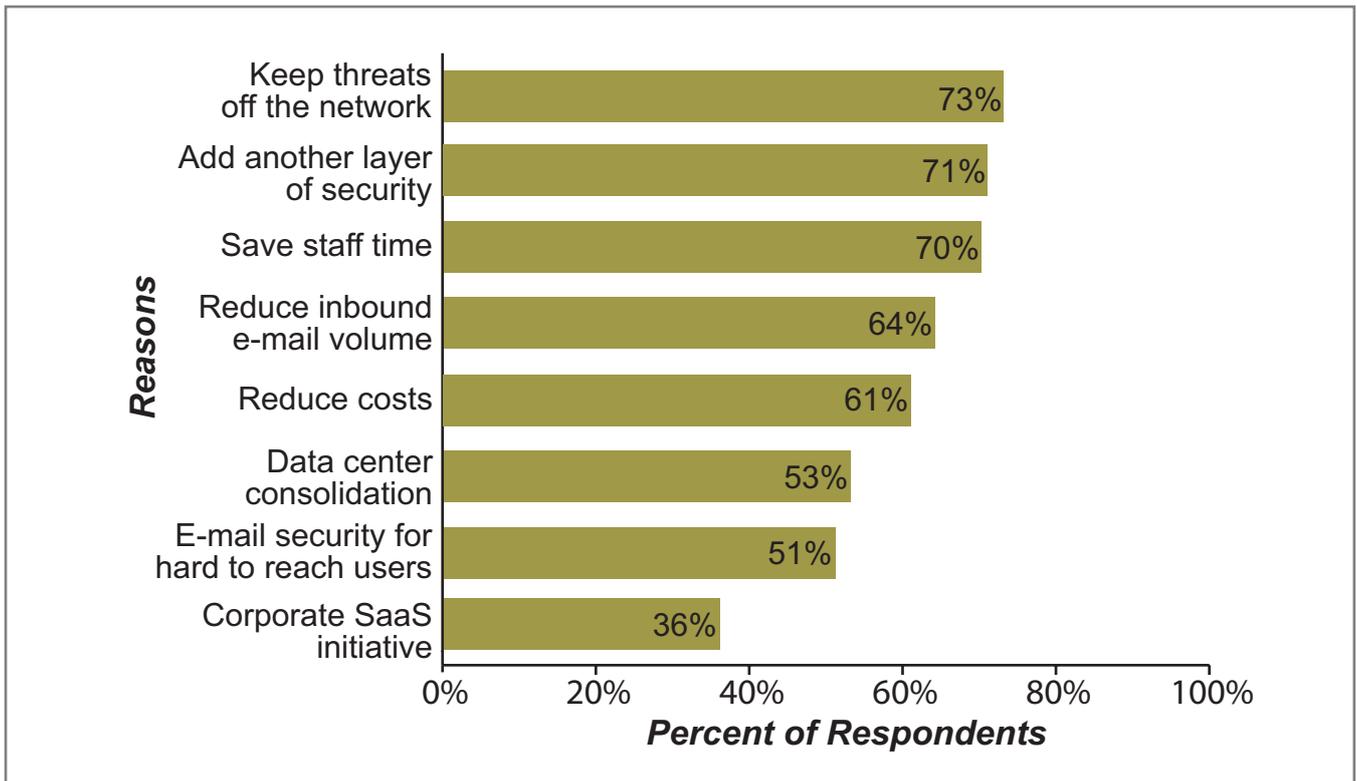


Respondent responses to the question: "What does your company use for e-mail security?"

This points to the nature of the buying process for e-mail security; many companies have a primary e-mail security solution, but will bolt on other solutions as needed. In some cases new solutions must be purchased to handle new threats not covered by existing solutions. In other cases there is an immediate capacity need, and there's no time to evaluate and buy new products, so hosted solutions make perfect sense. Mergers and acquisitions often leave enterprises with disparate mail security solutions as well. The cases are many and varied, but the end result is the same: rollout of hybrid e-mail security solutions has become a grass-roots movement.

As a follow-up to the question above, we asked respondents with hybrid solutions to choose from a list of factors that drove their deployments. Their responses boiled down to 2 key issues: increasing the level of security, and reducing the time/cost involved with deploying and managing e-mail security. It is clear that layering hosted/SaaS solutions on top of existing on-premise products is an additive solution.

HYBRID SOLUTIONS INCREASE SECURITY STRENGTH AND DECREASE WORKLOAD



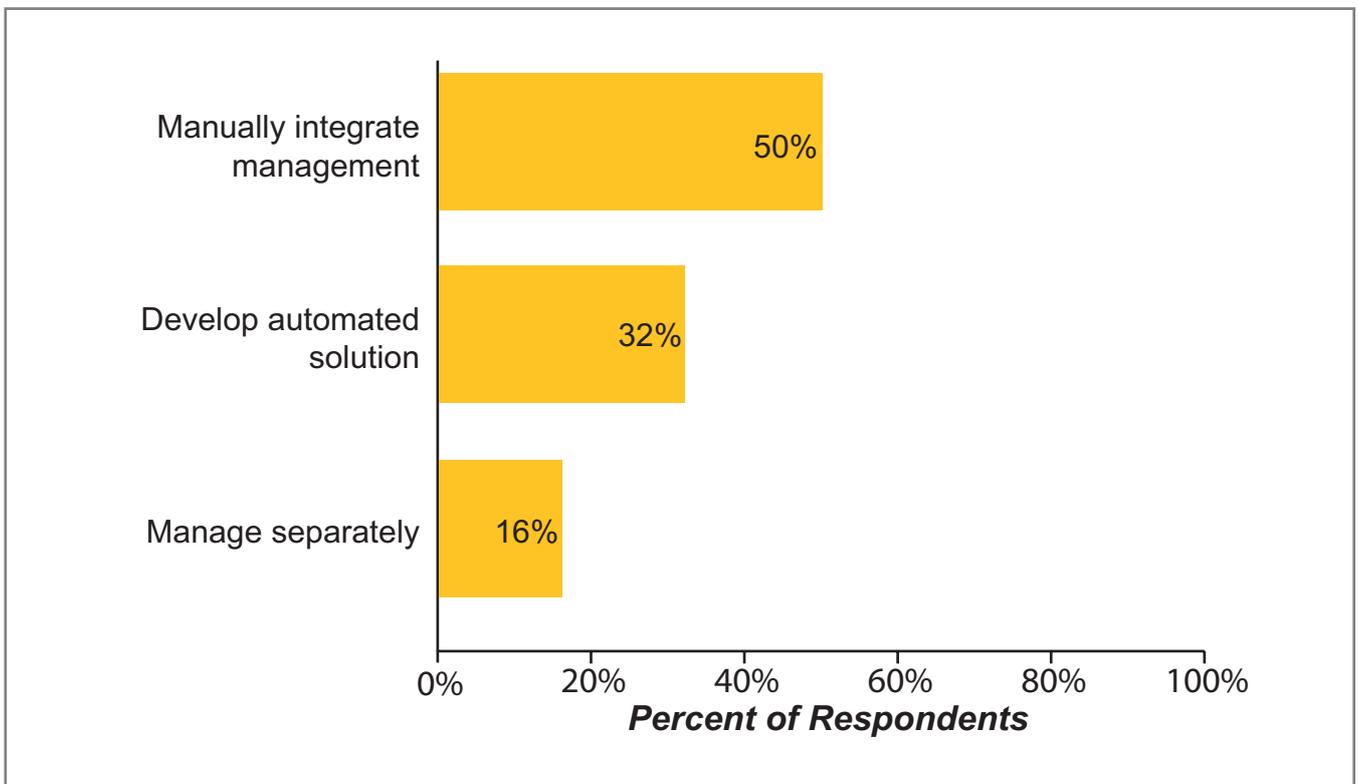
Respondent responses to the question:
 “Why did you choose to deploy hosted e-mail security in addition to on premises e-mail security products?”

The variety in the drivers above, and the strong responses for nearly all of them (other than corporate SaaS initiatives) is more evidence that companies will continue to deploy hosted e-mail security on top of an on-premise solution whether it’s in the plan or not, simply as a reaction to security events and capacity requirements.

So given that 46% of our respondents have deployed “do-it-yourself” hybrid solutions from multiple vendors, we wanted to understand whether the management and reporting is automated or manual, and among respondents managing them manually, if reporting is integrated. Most respondents manually manage their solutions and manually integrate reporting, or manually manage but don’t integrate; 32% of respondents use an automated solution.

This certainly creates a variety of challenges for IT departments. First, for those developing their own automated solutions, there is an investment in time and resources to develop and maintain that solution, which though functional, is probably missing many of the capabilities of their individual management and reporting tools for on-premise and hosted solutions. Respondents who integrate manually face the same issues as those developing their own automated solutions, but the problem is magnified, and respondents who don’t integrate management and reporting have no way to ensure that policies and security are consistent across their hybrid solution.

66% OF RESPONDENTS MANAGE HYBRID SOLUTIONS MANUALLY OR SEPARATELY



Respondent responses to the question: “How do you manage messaging policies, reporting, and message tracking across your layered hosted and on-premise e-mail security deployment?”

INTEGRATED HYBRID SOLUTIONS ARE THE KEY MOVING FORWARD

Looking forward, it seems logical that **integrated hybrid solutions from a single vendor**, offering one console for management, reporting, and administration of the SaaS and on-premise e-mail security, are critical in shoring up the leaks in hybrid solutions that many customers have built on their own.

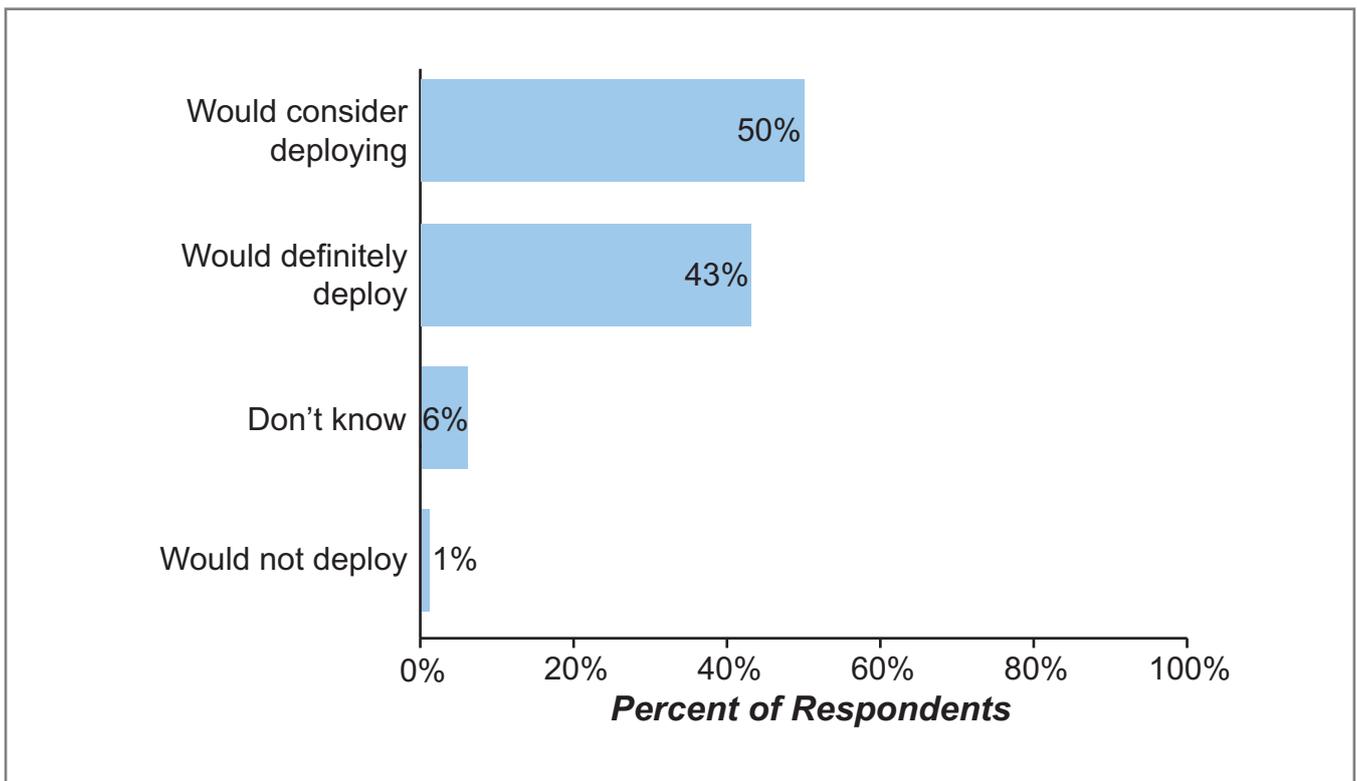
Integrated hybrid solutions with a single management console would alleviate many of the headaches of managing separate on-premise and SaaS solutions by:

- Providing a single location for managing quarantined messages
- Unifying message tracking capability
- Removing the need to manually build integrated reports for auditing/compliance issues
- Centralising all e-mail security policies

We asked respondents what they think about integrated on-premise/hosted solutions from a single vendor. Would they deploy if it were available, or is something else keeping them from looking at integrated solutions?

Respondents are nearly unanimous in their interest in integrated hybrid solutions, with **93% stating they would either consider deploying or would definitely deploy** (half said they would definitely deploy). As a follow-up, we asked in an open-ended question why respondents would deploy an integrated hybrid solution, and the responses were nearly all along the lines of, *it would be much more **cost-effective**, it would make management **easier**, and it would be **more secure**.*

STRONG INTEREST IN SINGLE-VENDOR INTEGRATED HYBRID SOLUTIONS

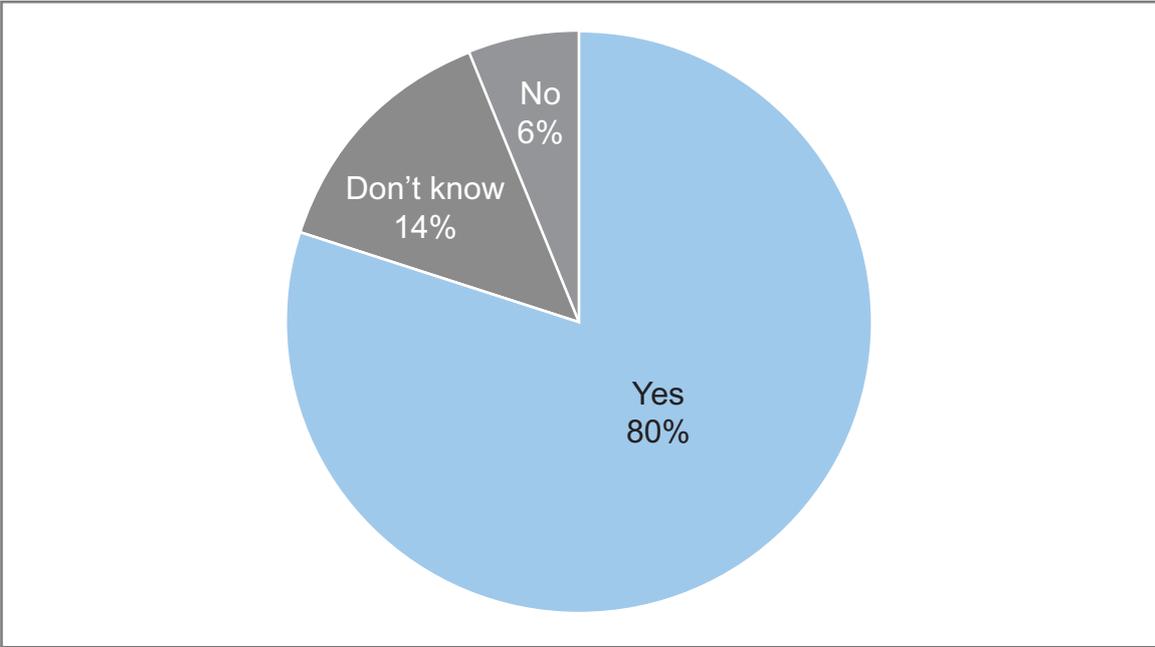


Respondent responses to the question:

"If it were available, would you purchase a solution that integrated deployment, management, and reporting for a hybrid e-mail security product that combined hosted e-mail security with an on-premise solution from a single vendor?"

To hammer the point home, we asked respondents if they believe that the cost (in time and resources) of deploying hybrid solutions for e-mail security could be significantly reduced if they purchased an integrated solution from a single vendor. Eighty percent of respondents said they do. Looking back at the question about how respondents currently manage hybrid solutions, it's easy to see why the cost savings could be significant.

RESPONDENTS THINK INTEGRATED SOLUTIONS MEAN SIGNIFICANT SAVINGS



REQUIREMENTS FOR INTEGRATED HYBRID E-MAIL SECURITY SOLUTIONS

That really leaves one remaining question: what should an integrated hybrid e-mail security solution look like? That question alone could be the subject of another full survey. Many vendors in this space are just starting to roll out their integrated hybrid products and there's no consensus yet on what makes a complete integrated hybrid solution, but there are some key components, such as:

- Common threat detection engine that works for both on-premise products and SaaS
- Common management platform that can either operate in the cloud or on-premise, or both
- Single source for policies that can be applied on-premise or in the cloud
- Simultaneous update of threat engines/databases for on-premise and hosted solutions
- Consistent user experience (interface, performance) for on-premise and hosted solutions

In short, the solution shouldn't force the IT department to make sacrifices when deciding whether a particular user or location is covered by an on-premise or hosted solution, it should simply be a matter of what makes the most sense from a deployment and cost standpoint. In the words of one of our respondents, "I'm interested in an integrated hybrid solution from a single vendor because it would make life a lot easier."

Hybrid on-premise and hosted e-mail security SaaS solutions are here to stay; now it's up to e-mail security vendors to offer integrated solutions so that IT departments can recover the time lost deploying and managing separate solutions, and improve their overall e-mail security posture.