EMAIL SECURITY'S
INSIDER SECRETS

There's more to email security than spam block rates.

Antivirus software has kicked the can. Don't believe it? Even Bryan Dye, Symantec's senior vice president for information security recently declared that "antivirus is dead." When antivirus software was first published by Symantec 25 years ago, it gave companies a great way to keep their computers and networks virus–free. A lot changes in 25 years, however. People who develop and distribute viruses adapted to antivirus software, rendering it ineffective.

A similar war has been waged between spammers and the email security industry. In order to keep spammers at bay, email security providers have continued to crank up security settings. Now, although as much as 99% of spam is stopped by most email security systems, a consequence of high spam block rates has risen to a new level of concern: false positives—email caught by spam filters that should have landed in your inbox.

Whether you have heard the term "false positive" before, if you work in IT, you've had to deal with them and you know that they cost you time and your company money. More than likely you've even spent hours sifting through spam folders and security settings to make sure people in your office actually get all the emails they want. Consequences of false positives can range from minor annoyances to major hassles and include losses in the millions of dollars.

If you're only comparing the spam block rate—and every email security provider will claim a very high rate—how do you differentiate between one provider and the next? Judge them by the false positive rate. Although measuring false positives is tough, it is the major differentiating factor between forward thinking email security providers and those that live in the past.

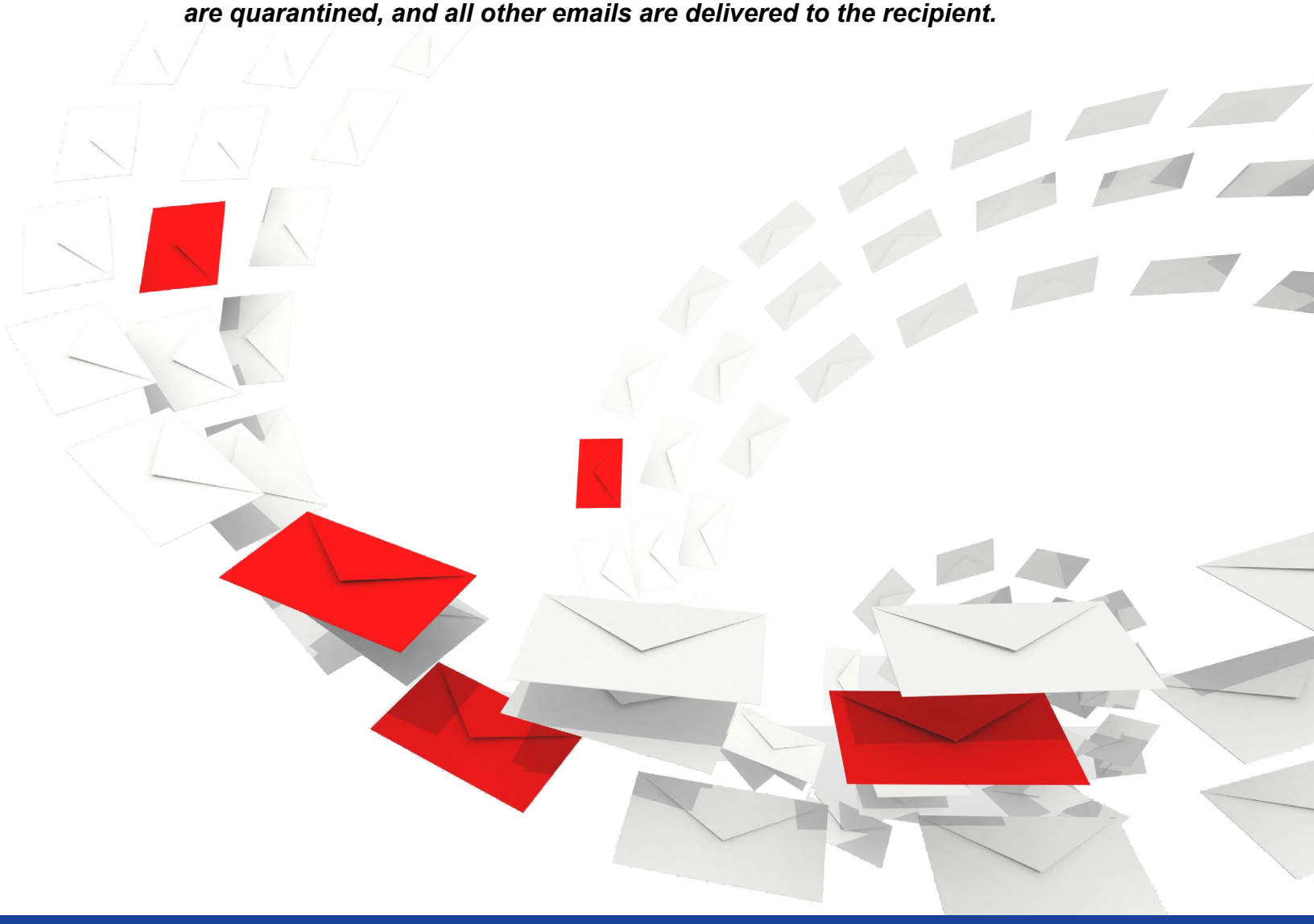
sendio®

Content Filtering

Email security tools that use a content filtering approach will scan the content of emails to look for patterns that are consistent with email spam. When the filter finds enough spam–like patterns, an email is prevented from landing in an inbox.

This is from a tech support manual for an email filtering solution. The same paragraph is in most email filtering manuals:

> ***Content filtering blocks email having content that indicates it is likely to be spam. The content of the message header, the message body, and attachments are examined. Many aspects of the content are ranked for probability of being spam then the rankings are added to determine if a user–selected threshold is exceeded. Emails with content exceeding the threshold are quarantined, and all other emails are delivered to the recipient.***



When you purchase traditional email filtering, a lot of what you are buying is the technology in content filtering attempting to squeeze out as much spam as possible. Heuristics and Bayesian methods are used to create complicated algorithms that block spam without causing too many false positives. Both are used to model complex systems in fields like disease control, psychology, and finance. Compared to the big problems of these fields, filtering email spam seems like a much more modest endeavor, yet it presents an overwhelming challenge because of the pace at which spammers adapt to the filters.

Spammers test their emails against content filters to make it difficult for the filter to distinguish between legitimate email and spam. In order to block emails from these clever spammers, you need to crank up your filter settings. The problem is that the more you crank up those settings, the more false positives you will experience.

"An IT guy's worst nightmare."

Don't believe this stuff matters? One Colorado law firm missed a court date because their spam filter prevented them from receiving emails from the U.S. District Court of Appeals.

Because of the missed court date, the law firm was required to pay attorney fees and expenses of the firm on the other side of the case.

You can read about it in the Washington Post.

Costly False Positives

Depending on the email filter, any email could incorrectly be classified as spam. There are some, however, that are more likely than others to be unjustly banished to the spam folder. These tend to be emails that you don't get all the time. Some are automated messages. Here are a few types of emails that tend to fall prey to spam filters:

- **Tax documents**
- **Health records**
- **Court notices**

What else do emails like these have in common? **You would never want to miss even one of them.**

If even the most advanced content filtering algorithms can't stop spam **and** make sure you don't miss important emails, where should an IT administrator or executive turn?

A Better Way to Filter

When you're talking to someone, how well you know that person plays a big part in determining how much you'll listen to what he has to say. ***Its common sense: You listen to people you trust.*** So why does content filtering ignore common sense? It basically ignores who is trying to communicate with you to focus on what they are saying.

Think about it: If a doctor you know sends you records from your recent trip to the hospital, you would immediately trust her. Whatever she tells you—no matter how unusual it is—is something you want to listen to because she is someone you trust. If you filtered your conversations by content, though, you might hear her say something unusual and then stop listening. This is how content filters work. As a result, they classify medical records as spam more frequently than you might imagine just because they "look or say something different" than normal emails.

It is time for your email security provider to use some common sense. Instead of only evaluating an email to determine if it is spam or not, why not also evaluate the sender?

The best modern email security providers introduce some common sense and ask "Can this sender be trusted?" In the world of email security, you have to use different cues than the ones you use when talking to someone face to face, but the principal is the same—it's just a matter of identifying the right cues.

Sendio: Reclaim Your Inbox

When you talk to someone, you ask yourself questions like these to figure out how much you trust what this person tells you:

- **Do you know this person?**
- **What is this person's reputation?**
- **How does this person present himself?**

Your email security provider should be evaluating the trustworthiness of the email servers and people that send you email. Sendio uses two tools that incorporate contact–based email filtering: Sendio's Email Security Gateway™ and Sendio's Opt–Inbox™.

Sendio's Email Security Gateway

Silverlisting™, a part of Sendio's Email Security Gateway™, gathers key information that is used to determine whether email senders are trustworthy. It works like this:

1. **A sender attempts to send you an email.**
2. **The email enters the Sendio Email Security Gateway™.**
3. **Sendio uses a SMTP deferral code to determine the authenticity of the sender.**
4. **Based on the information the sending mail server sends back, Sendio can determine if the email was from a spammer or from a legitimate sender.**

Silverlisting allows Sendio to instantly evaluate the trustworthiness of email servers that send you email.

Sendio's Opt–Inbox™

Sendio has flipped the tables on senders of bulk mail and spam. Sendio's Opt–Inbox™ makes it possible for you to opt in to email lists so you'll never have to opt out of email you don't want to receive ever again. Here's how it works:

Sender Address Verification™ (SAV) – Sendio's SAV is the heart of the Opt–Inbox™ solution. Sendio's Opt–Inbox™ verification process distinguishes humans from automated senders, ensuring Sendio users receive only the email they want.

Sendio Queue – Built for the enterprise, the Sendio queue is a repository for email that you may want later but don't want now. This customizable queue allows you to organize newsletters, bulk mail, and discounts, as well as manage your contacts. The Sendio Queue allows users to view, accept, drop, and delete messages that have not successfully passed the SAV process. Additionally, the Queue allows users to add and remove senders in their community, meaning that you'll have access to machine created messages such as bacn, bulk mail, and newsletters without clogging your inbox.

Email Address Community – Because your Opt–Inbox™ concentrates on trusted communities to build your email list, you'll know that everyone in that community is seeking a real conversation. Build your community through outbound messages and watch as the SAV takes care of the rest.

sendio®

About Sendio

Sendio offers solutions to enterprises and institutions that will increase employee productivity while eliminating spam and malicious emails.