

# TotalBlock: New Challenge/Response Anti-Spam Technology

The world of anti-spam technology encompasses many different techniques. Common ones include:

- Blacklisting (look up a sender against a list of known spammers, usually by IP address range). The list is typically maintained by the network administrator.
- Whitelisting (look up a sender against a list of known “friends”). The list is typically maintained by the user.
- Bayesian filtering (filter against a list of “good” and “bad” words). The list is automatically maintained, led by the user’s example. The system watches the user’s response to incoming messages, specifically whether the messages get flagged as spam or not.

A strong technological response to spam continues to be important, even after the advent of legal weaponry, such as CAN-SPAM and the European Privacy Directive.

## *Challenge/Response and TotalBlock*

There’s a less well-known technological approach to stopping spam, which can be very useful and appropriate for some environments. This is known as “Challenge/Response” (C/R).

A C/R spam control system automatically maintains the whitelist. An incoming message is examined to see if the sender is already on the list. If so, the message is delivered as normal.

If not, the system will automatically reply to the sender, so that they can prove that they’re a real person, and not a spammer’s bulk sending tool (the automatic reply is known as the *challenge*). The “proof” (or the *response*) is usually requested in the form of a reply back to the C/R server, or by clicking on a web link.

Once the proof has been satisfactorily received, the message can be delivered. The sender’s address gets automatically saved to the whitelist for future use.

You need to think carefully before employing C/R to protect the mailboxes of customer-facing roles, such as customer service. Unless you already know your customers' registered email addresses, you may conclude that you do not wish to reject customers' mail.

Compared to other approaches, C/R can be much easier to implement and administer, reducing your costs. However, you want to make it as easy as possible for customers to do business with you. Making customers prove their humanity before being able to communicate with a supplier can be too much of a barrier.

Recipients also need to be aware that bona-fide mailing list email will probably get blocked, since the sending email address often won't be able to respond to a challenge

C/R technology has existed since at least 1996, but hasn't enjoyed wide uptake for reasons we'll talk more about later.

### ***Strengths of the Challenge/Response Approach***

C/R has its advantages, when correctly used:

- Blocks 100% of spam.
- Also blocks email-borne malware, such as viruses and worms.
- No "false-positive" problem.
- Server-based C/R needs no client-side software installation.
- No filter updates required.
- Requires very little overhead from IT administrators or users.

### ***New Millennium and TotalBlock***

New Millennium Solutions (NMS), an Australian company, have a C/R technology they call TotalBlock. Unlike other C/R implementations, the initial whitelist lookup is performed before the message itself is actually received. If the lookup fails, the message receipt is optionally aborted; saving the incoming bandwidth that otherwise would have been consumed.

While rejecting spam before it's been received makes TotalBlock stand out from the other C/R solutions, this is a configurable option. Some organizations may choose for the message to be received and quarantined.

In addition to the above list of C/R benefits, TotalBlock:

- Saves inbound bandwidth which allows management of high volume periods. Also useful if your ISP charges by data volume (as is common in Australia).
- Is integrated with Windows domain security.
- Exposes detailed logs and statistics.
- Allows users to temporarily suspend blocking from unknown senders, via a web interface.

### ***TotalBlock Future Development***

NMS have a roadmap for future releases of the TotalBlock product, including these ideas:

- The TotalBlock whitelist is stored in an internal database. Some customers will wish to use a database with which they're already familiar. NMS will be providing the option to use other databases.
- Similarly, some customers will wish to store the whitelist in a pre-existing LDAP tree. This option is planned for a future release.
- TotalBlock currently runs on Windows servers. Future versions will also run on Unix and Linux.
- In a future release, administrators will be able to set a policy to disallow users from turning off or suspending the blocking of possible spam.

*Author: Richi Jennings  
Editor: David Ferris*

### ***Bulletin Sponsored by TotalBlock***

TotalBlock commissioned this bulletin with full distribution rights. You may copy or freely reproduce this document provided you disclose authorship and sponsorship and include this notice. Ferris Research independently conducted all research for this document, retaining full editorial control.

### ***Ferris Research***

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and Asia/Pacific.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit [www.ferris.com](http://www.ferris.com) or call +1 (415) 986-1414.

### ***The Ferris Research User Panel***

The User Panel consists of IT professionals who work with messaging and collaborative technologies, providing services to staff of their organization. People join to share experiences with other people like themselves, learn from each other, and keep current on news and trends.

If you provide technical support for an email system, and you are not a member of the User Panel, you can join and learn more about the User Panel at <http://www.ferris.com/url/userpanel.html>. There is no charge to join.