



Anti-spam Alternatives

Today, there are 4 different types of Anti-spam tools available in the market. The benefits and disadvantages of each alternative are summarized as follows:

Alternative 1. Desktop Anti-spam

A copy of the Desktop Anti-spam Anti-virus tool is installed on each user's desktop. Scanning for viruses and filtering of spam emails are done with the desktop's CPU power. Users may experience slow downs or interruptions when filtering occurs. Cost is based on a per-user license. This alternative offers a cost benefit when user volume is low but becomes expensive as the number of users increases. Similarly, the Administrator's workload related to upgrading and maintaining individual copies of software on desktops becomes unacceptable as the number of users increases.

Alternative 2. Server-based Anti-spam

The spam filtering software is installed on the email server, e.g. Exchange Server or on the gateway. While this alternative avoids having to buy more hardware, its major disadvantage is that the installed software will consume the email server's CPU power and degrade the email server's performance. **Some of these server-based anti-spam tools actually recommend that users avoid scanning installed directories and IIS directories.** Maintenance is another factor as program removal and software updates may not be that straight forward.

Alternative 3. Appliance-based Anti-spam

This is a turnkey solution. It eliminates the waste of email server CPU cycles for anti-spam and anti-virus functions. Generally, the Appliance solutions are feature-rich and easy to install. However, hardware reliability becomes an important factor as a faulty Appliance could stop all emails and block traffic. It is recommended that the Appliance support the pass through mode so that email traffic can still pass through if the Appliance fails. **Currently Europa is using this method.**

Alternative 4. Outsourced Anti-spam

Companies may outsource their Anti-spam functions to a Service Provider. However effective this may be, it could introduce two fundamental flaws:

- Inefficiency
 - Emails between internal users still go through the Service Provider and the Internet. This could introduce delays due to network traffic.
- Security Breach
 - Emails, including confidential and restricted, are stored at the Service Provider's location.
 - Emails are stored in plain text. Email protection is only as good as what the Service Provider can provide.