Comparative Performance of Anti-Spam Gateways

Joel Snyder
Opus One
January, 2012

In Gartner's August, 2011 "Magic Quadrant for Secure Email Gateways," the analysts suggest that the anti-spam market is mature and that products are not differentiated based on their spam-filtering effectiveness. This statement is not entirely correct. In fact, there are significant differences in the underlying anti-spam engines used by each of the significant vendors, and all anti-spam products are *not* equal from the point of view of their ability to filter spam.

Opus One has performed monthly efficacy testing on anti-spam products for over six years. Our unique and industry-leading methodology relies on actual corporate mail streams, manually analyzed for spam and non-spam email, run for approximately one week out of each month. This is a laborious process, but it provides significant real-world results--which differ from results obtained through automated tests based on artificial mail streams.

In December, 2011, Trend Micro asked Opus One to test products from the nine vendors identified by Gartner as Challengers or Leaders in the field (Barracuda Networks, Cisco, Google, McAfee, Microsoft, Proofpoint, Sophos, Symantec, and Trend Micro). Comparing results from different products is not simple, because all products have a wide variety of configuration options, including sensitivity and use of reputation services. The results shown here are from the most common configuration options for each product, but do not include individual end-user tuning (such as use of personal address books to safe-list addresses).

In the graph below, the products from the nine Gartner-identified vendors are compared for their spam catch rate (sensitivity) and false positive rate (positive predictive value). The products in the graph are not identified by name, except for Trend Micro, which had the highest spam catch rate at 98.06%.