

# Cloudmark, Inc.

## Cloudmark Authority™

### for Service Providers

#### Anti-spam Effectiveness vs. Symantec Brightmail Anti-Spam Version 6.0



Test  
 Summary

**Premise:** Gateways designed to thwart phishing attacks, viruses and E-mail spam must be able to deliver exceptionally high rates of spam blockage combined with low levels of false positives to be effective to service providers and enterprise networks. Those anti-spam/anti-virus products that deliver premium performance along with efficient hardware utilization will offer true one-stop shopping for service providers.

Cloudmark, Inc. commissioned The Tolly Group to measure the effectiveness of the company's Cloudmark Authority™ for Service Providers at blocking spam and guarding against false positives.

Tolly Group engineers tested the performance of Cloudmark Authority against Symantec Brightmail Anti-Spam Version 6.0. In accordance with The Tolly Group's Fair Testing Charter, Symantec was invited to review the test methodology, offer suggestions for optimal configuration of its product and review/comment on its test results.

Engineers measured the percentage of spam blocked by the tested devices, and the percentage of false positives to determine the relative effectiveness of the products at fighting spam.

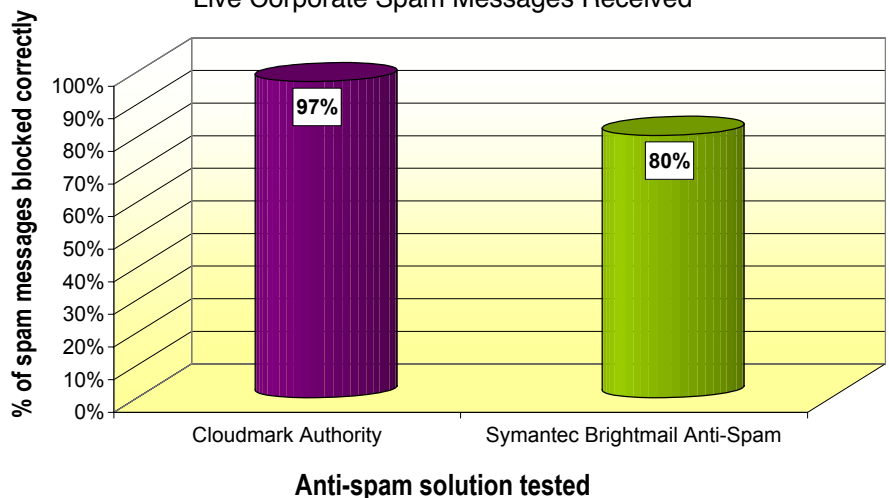
Tests were conducted in July and August 2006.

#### Test Highlights

- ▶ Blocks 97% of 44,288 inbound messages containing spam, while Brightmail Anti-Spam misses 20% of incoming spam
- ▶ Demonstrates that it is 100% effective at guarding against false positives
- ▶ Offers one-stop shopping for protection from E-mail abuse by integrating anti-virus, anti-spam and anti-phishing capabilities into a single product

#### Spam Detection Percentage of Cloudmark Authority vs. Symantec Brightmail Anti-Spam

Based on 44,288 Service Provider Honeypot and Live Corporate Spam Messages Received



Source: The Tolly Group, August 2006

Figure 1

## Executive Summary

Tests show that Cloudmark Authority is 21% more accurate at blocking spam than Symantec’s Brightmail Anti-Spam and did not generate any false positive messages.

Service providers and enterprise network architects can benefit from adoption and deployment of integrated tools that offer protection from E-mail abuse. Cloudmark Authority for Service Providers bundles support for anti-spam, anti-virus and anti-phishing into a single product.

This test focuses on Cloudmark Authority’s anti-spam effectiveness, particularly when compared to Brightmail Anti-Spam.

Cloudmark Authority correctly identified and blocked 97% of spam messages it encountered while Symantec Brightmail Anti-Spam blocked 80%.

### SPAM DETECTION

Engineers measured the ability of Cloudmark Authority for Service Providers and the competitive product tested to detect incoming spam with accuracy and to correctly block identified spam messages.

Tests show that out of 44,288 service provider honeypot and live corporate spam messages received, Cloudmark Authority blocked 97%, or 42,931 spam messages.

By contrast, the Symantec Brightmail Anti-Spam blocked 80%, or 35,609 spam messages, incorrectly allowing 8,679 spam messages to

pass onto users. (See Figures 1 and 2.)

This demonstrates that Cloudmark Authority is 21% more effective at blocking spam than Symantec Brightmail Anti-Spam. Such a spam blockage rate, as exhibited by Brightmail Anti-Spam, is unacceptable for service provider and enterprise-class scenarios where accuracy is a high priority.

For service providers, blockage of spam is essential because it translates into an infrastructure capacity issue. The percentage of spam versus legitimate E-mail is increasing and is inhibiting the service provider’s ability to support more users and offer larger, more competitive mailbox sizes.

For enterprise-class users, spam blockage is important because it hits enterprise IT where it hurts the most — in

| Spam Processing Analysis of Cloudmark Authority versus Symantec Brightmail Anti-Spam |           |            |
|--|-----------|------------|
| Category   | Authority | Brightmail |
| Total Inbound Messages Tested*   | 45,705    | 45,705     |
| Total Spam   | 44,288    | 44,288     |
| Spam Blocked Correctly   | 42,931    | 35,609     |
| Spam Detection Rate  | 96.9%     | 80.4%      |
| False Negatives (Spam Missed)  | 1,357     | 8,679      |
| False Positives Percentage (Classified as Spam but Not actually Spam)                | 0         | >0.01      |

\* NOTE: For the test, E-mail messages were collected for a four-day period from July 25th to July 28th. The messages include honeypot messages which were directly sent from a Tier 1 Service Provider, plus real-world Tolly Group corporate E-mail messages.

the wallet. Excessive spam results in lost productivity as users sift through inboxes for legitimate messages.

**FALSE POSITIVES**

When an anti-spam product incorrectly identifies legitimate incoming E-mails as “spam” and then blocks those messages, the product is guilty of creating “false positives.”

With 45,705 messages sent, Cloudmark Authority experienced a false positive rate of 0%.

**METHODOLOGY & CONFIGURATION**

Tolly Group engineers tested Cloudmark Authority Cartridge version (3044.1.0.12) against Symantec Brightmail Anti-Spam version (6.0.3.05) using out-of-the-box standard configurations.

**TEST BED CONFIGURATION**

Tolly Group engineers ran Cloudmark Authority and Symantec Brightmail Anti-Spam on the same mail gateway server. Both anti-spam services were installed on a Hewlett-Packard Co. ProLiant ML370 server with two 2.8-GHz Intel Xeon single-core processors and 2-GB of RAM. The server was configured with RAID 1 (mirrored) – 200-GB usable space but 400-GB total hard drive space. The operating system installed was CentOS version 4.3 (Linux).

Testing was conducted during four days – from July

25th through July 28th – using a Tier 1 service provider’s honeypot accounts and live E-mail traffic from The Tolly Group production environment. The service provider forwarded 300 randomly selected honeypot accounts to a Tolly Group test E-mail account. In all, 45,705 messages were handled by the devices under test, including legitimate messages and spam.

All messages used for the test were scanned by each spam filtering solution in parallel. The real-time stream of messages was “mirrored” to both solutions for scanning; meaning that both anti-spam solutions received exactly the same live messages. A Tolly Group test E-mail account from the “@tolly.com” domain was utilized to receive all incoming messages from the honeypot accounts in order to avoid any issues that could arise to The Tolly Group E-mail infrastructure. A custom-made script was created to allow each solution to tag the message header with a “spam” or “clean” classification based on each solution score.

Each anti-spam solution, by default, has a minimum score threshold to classify whether or not a message is spam. Engineers used the default (out-of-the-box) settings for both solutions. Cloudmark Authority uses 96 as a minimum score for

Cloudmark, Inc.



Cloudmark Authority for Service Providers

Anti-spam E-mail Effectiveness

**Product Specifications**

*Vendor-supplied information not necessarily verified by The Tolly Group*

Cloudmark, Inc.  
Cloudmark Authority

**Capabilities**

- Most accurate in anti-spam, anti-phishing & anti-virus
- Near wire-speed filtering
- 90% reduction in CPU requirement

**Technology**

- Intelligent message fingerprinting
- World’s largest threat detection network
- Trust evaluation system

**Benefits**

- **Real-Time Threat Response.** Cloudmark Authority detects emerging threats faster than any other solution
- **Unmatched Accuracy.** Cloudmark wins 100% of competitive service provider accuracy trials. Due to global feedback and language-agnostic analysis, Cloudmark stops spam in all languages
- **End-to-End Protection.** Cloudmark Authority offers complete protection against all forms of messaging abuse over both wireline and wireless networks
- **Operational and Infrastructure Savings.** Cloudmark Authority delivers 10-15x faster messaging throughput than competitive solutions while utilizing 90% less CPU.

**For more information contact:**

Cloudmark, Inc.  
128 King St.  
San Francisco, CA 94107  
Phone: (415) 543-1220  
Fax: (415) 543-1233  
<http://www.cloudmark.com>

classifying “spam,” while Symantec Brightmail uses 90. Any message with a score in between the minimum

score and 100 was considered spam. Any messages that exhibited a different classification (such as a “spam” tag

from Authority or a “clean” tag from Symantec) from each anti-spam solution were saved into a separate directory for manual classification and verification. The manual classification was done in order to determine the false positives and/or false negatives found on each anti-spam solution. Engineers also designated two more folders, named “both spam” and “legit”, for those messages classified as spam for both anti-spam solutions and legitimate messages coming from the honeypot server to the test mail account respectively.

The system was configured to look at all messages that connected to the email system. Some systems attempt to utilize Real-Time Blackout lists and connection dropping techniques to enhance their effectiveness. This test configuration was designed to look at a ‘raw’ feed of messages to the Tolly Group systems. The accuracy rates are based on the effectiveness against all traffic presented to the system. Brightmail has RBL-based content filtering built-in and its results reflect the benefits of RBLs while Cloudmark’s does not.

**ANTI-SPAM TEST PROCEDURE**

Once messages were scanned by each solution, they were filtered out by the script and segregated into four categories that then were stored or delivered based on the tag header of each message. The

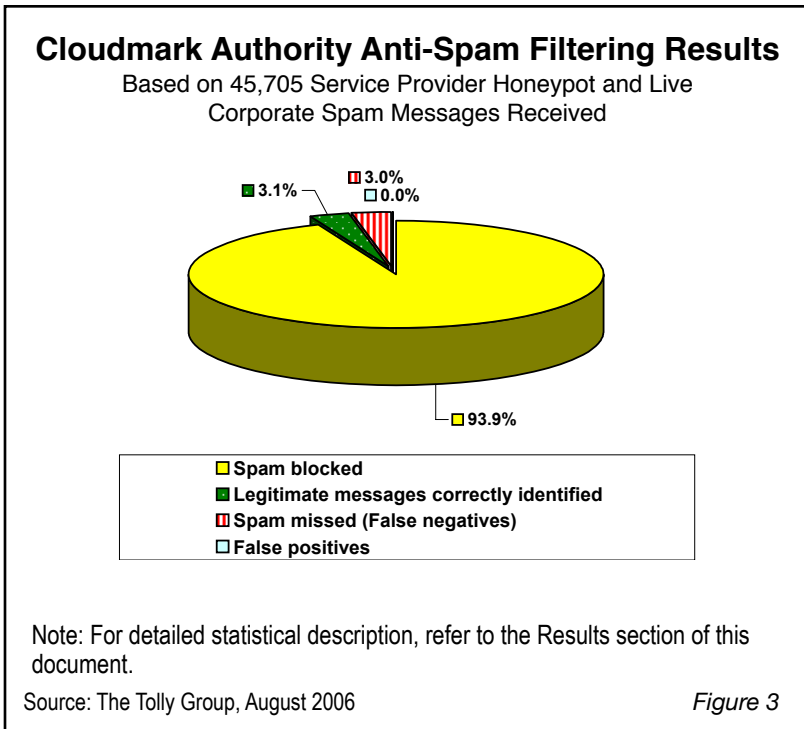


Figure 3

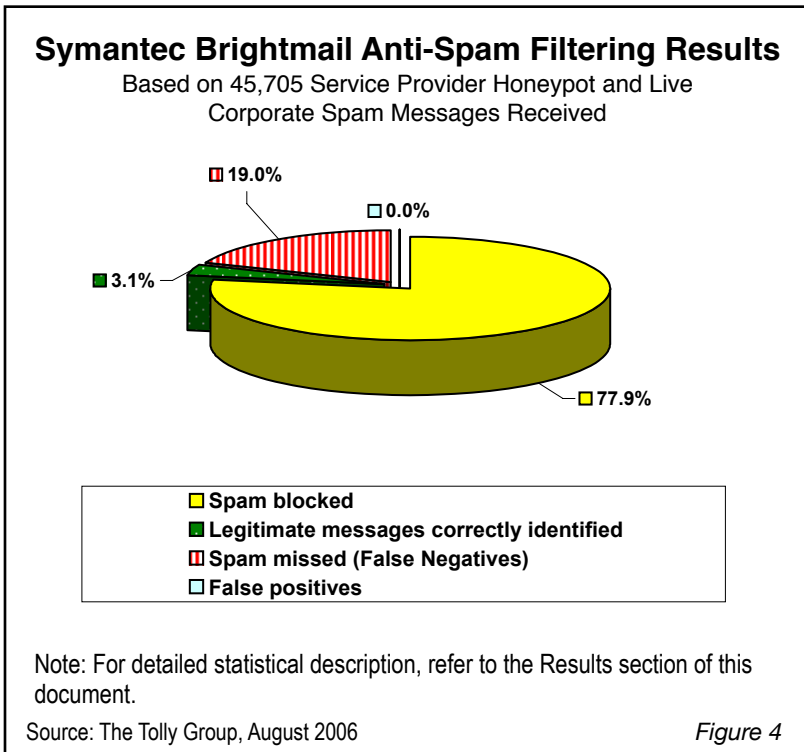


Figure 4

four categories were: (1) both spam, (2) Authority “spam only”, (3) Brightmail “spam only” and (4) legitimate.

Any messages that both anti-spam solutions agreed to be spam, were stored in a directory named “both spam”. Any messages with a differing score by the two anti-spam solutions were classified as spam and stored in two separate “spam only” folders for the respective solutions. The only messages classified as “legitimate” by both solutions were delivered to respective Tolly Group mail accounts. Lastly, any legitimate message coming from the honeypot server to The Tolly Group test account was stored in a “legit” folder in the E-mail gateway server for manual classification.

For the manual classification, engineers utilized a Mail User Agent (MUA) — Novell Evolution version 2.0.2, which came as an add-on program in the operating system, that supports opening mailbox files from a directory, to manually look through the “spam only” messages from both solution folders, and check the honeypot legitimate messages folder, as well. During the manual classification, engineers determined whether messages were “unsolicited” or not by checking the following message criteria: porn, sex, illegal prescription drugs, gibberish language, “no page found” hyperlinks, no content, etc.

Engineers concluded that any message with a differing score from the two anti-spam solutions was counted as a false negative for the other solution after manually checking that it was actually spam. For false positive messages, engineers manually checked for any legitimate message being classified as spam under both anti-spam directories.

The number of total inbound messages tested was collected during four days which included honeypot messages sent from a Tier 1 service provider to a Tolly Group test account and Tolly Group corporate mail. The number of total spam was gathered from the sum of all spam messages detected by Cloudmark Authority and Brightmail — 42,931 and 35,609, respectively, plus the spam missed (false negatives) by the two solutions — 1,357

and 8,679, respectively. The number of false negatives was obtained from the number of spam messages missed by the two solutions — Authority 1,357 and Brightmail 8,679 — and the number of spam messages received by Tolly Group employees’ mailboxes — 29 messages, plus the number of spam messages received on the honeypot legitimate mailbox folder on the mail gateway server — 146 messages.

The number of false positives was obtained from the number of spam messages classified as “spam” by the two solutions but it was not actually spam after engineers manually checked each message. For Cloudmark Authority and Brightmail anti-spam solutions, the number of false positives was 0 and 1, respectively.

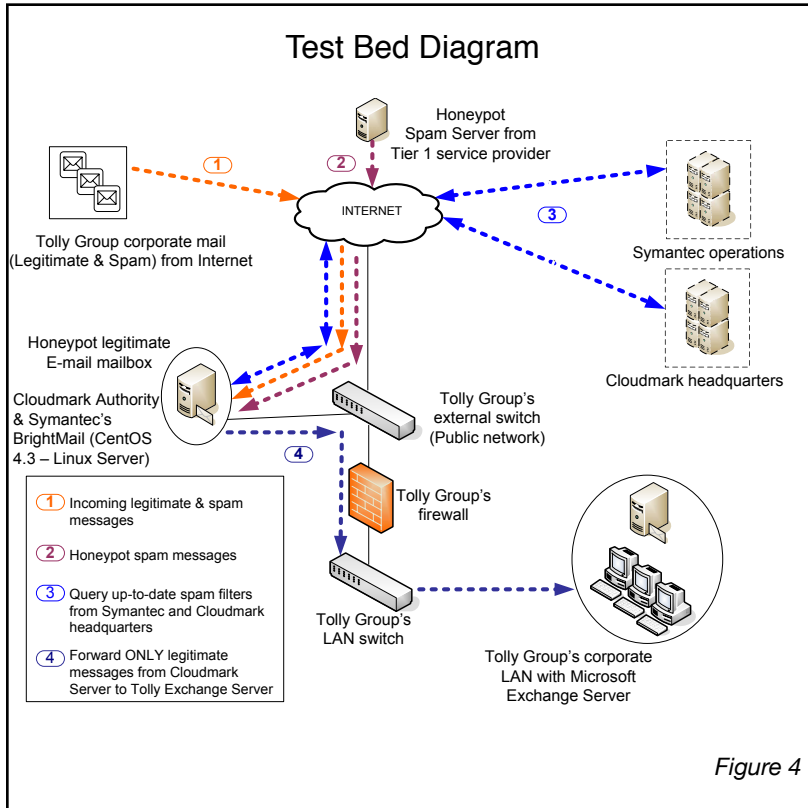
### Fair Testing Charter™ Interaction with Competitors

The Tolly Group contacted Symantec in June 2006 and several times during August 2006 when tests were ongoing. Symantec was invited to review the test plans, the product levels and configurations of the company’s products and to review and comment on results specific to Symantec’s product. On August 10th, a Symantec representative requested the product test results.

On August 18th, Carlin Wiegner, VP Messaging & Web Gateway at Symantec raised issue with the four-day length of the test, “While longer is clearly better, I never green light reviews under one week,” he said. The Tolly Group explained that message volume of 45,000 messages, and not test run time, was the key factor in determining anti-spam effectiveness.

For more information on this process, please see: <http://www.Tolly.com/FTC.aspx>.





The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.



The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at <http://www.tolly.com>, [sales@tolly.com](mailto:sales@tolly.com)

## Test Equipment Summary

The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

| Vendor                      | Product              | Web   |
|-----------------------------|----------------------|---|
| Aten International Co. Ltd. | ALTUSEN Model # KH88 | <a href="http://www.aten.com">http://www.aten.com</a>     |
| Novell, Inc.                | Evolution Ver. 2.0.2 | <a href="http://www.novell.com">http://www.novell.com</a> |

## Terms of Usage

**USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.**

*This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.*

*This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document*

*The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.*

*When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.*

*All trademarks are the property of their respective owners.*