

## THE ECONOMIC IMPACT OF MESSAGE FILTERING ACCURACY

November 2006

### ABSTRACT

Service providers often think that their current message filtering solution is “good enough.” Next generation systems may increase accuracy by a few additional points, but a few points of improvement will not make a big difference in stopping email abuse, they conclude. In reality, even a small improvement in filtering accuracy can make a big difference for service providers and subscribers.

Today spam, virus, phishing, spyware and other types of attacks are revolutionarily different than they were just 12 to 18 months ago. While vendors have concentrated on innovative advancements in messaging security, innovations have also been occurring in attack technologies.

In fact, 90-96% of all service provider email traffic is abusive, according to measurements from Cloudmark’s Global Threat Network, which processes over 3 billion message per day. Over 90% of these messages are generated by zombies and botnets. And new virus attacks cause their maximum damage in their earliest stage of spreading.

We will discuss how every percentage point increase in messaging filtering accuracy actually does have a significant impact on infrastructure and operational costs as well as the subscriber experience.

### THE IMPORTANCE OF FILTERING ACCURACY

The highest level of filtering accuracy has never been more critical due to these factors:

- Both the volume of mail to be processed and the volume of spam have increased
- More mail storage is available, which can be filled with spam
- Since subscribers expect service providers to solve the spam problem, poor filtering affects customer satisfaction

Traditional heuristics or statistical-based filtering systems are somewhat successful at stopping attacks using known techniques. For new attacks, however, these systems rely on research teams to identify the attack, design a solution to block the attack, test the solution against thousands of existing rules and then deploy the solution to their user base. Since this process is a manual, it usually means hours and days before the attack is stopped during which time the spam, virus or phishing campaign inflicts its maximum damage.

When considering improved accuracy, the timeliness of that accuracy is also a key factor. For example, every anti-virus vendor can prove a 100% accuracy rate over time; however, that rate is only relevant when the blocking occurs early, before maximum damage is done. Accuracy should not only be measured in terms of whether something is blocked, but also when blocking starts and how well the blocking works against attack mutations.

### THE COSTS OF POOR FILTERING

Please refer to Cloudmark’s comprehensive Message Filtering ROI Model for more detail. Briefly, here are some of the cost reduction benefits resulting from improved filtering accuracy.

#### Infrastructure Costs (CAPEX)

Reduction in the number of edge MTAs or appliances. This saving is primarily due to the lightweight nature of next-generation scanning techniques which require only minimal processing per message. When compared to traditional rules-based systems, which are inherently resource-intensive, advanced fingerprinting techniques such as those used by Cloudmark,

---

demand far less processing power.

**Reduction in storage** Delivery of spam can be very costly. Because spam represents up to 96% of all messages delivered to a carrier, a low catch rate can mean the system delivers more unwanted emails than legitimate emails. Improving a catch rate by 10% can reduce the delivery and storage of messages up to 50%.

**Reduction in number of internal mail servers and Webmail/POP/IMAP servers** Internal mail servers are another expensive element in the mail service infrastructure. Costs per server range from \$10,000 to \$80,000, plus 10% or more in annual maintenance. A 10% increase in accuracy means up to 50% reduction in the messages per day that the internal mail server needs to process.

**Reduction in bandwidth** Spam messages usually range from 15KB to 25KB in size, although recent flooding of image spam significantly raises that. A 10% improvement means up to 50% lower bandwidth consumption for POP/IMAP users, freeing up precious core network infrastructure to be used for revenue-generating services.

**Trojan/zombie attacks** In determining bandwidth savings from accuracy, one must consider spam that originates from within the user base by spammers or zombie/botnet attacks. Spam originating from the service provider's network introduces the possibility of users, or even the mail platform, being blacklisted leaving subscribers with rejected mail. This situation has both a financial and customer satisfaction impact. While there is not enough substantial data for cost calculation in this area yet, next-generation solutions filter outbound email and help identify zombies within the service provider network.

#### Infrastructure Costs (OPEX)

OPEX savings resulting from improved accuracy include significantly fewer servers and fewer people needed to manage them on an ongoing basis.

#### FILTERING ACCURACY AND CUSTOMER SATISFACTION

Three factors negatively affect customer experience: 1) missed spam, 2) false positives, and 3) a feeling of helplessness to correct the problem.

**Missed spam** Users see and must act on spam that shows up in their inbox. To them, it is a reflection of the service provider's ability to provide a good service. Bad filtering often reflects poorly on the service as a whole. User dissatisfaction increases dramatically with failed spam filtering. A 10% point increase in accuracy translates to between 2 times and 3 times fewer spam messages getting through to the inbox. This directly translates to lower spam-related support calls. Customers have reported a 90% drop in spam-related helpdesk calls after a Cloudmark rollout.

**False positives** False positive rates have an equally significant impact on customer satisfaction and the perception of the quality of service. Finding even one legitimate or critical message in a spam folder dramatically degrades the user's confidence in the service provider's ability to competently filter messages. False positives are more likely to generate helpdesk calls. The most common user request is to turn down the aggressiveness of filtering or to allow users to add their own "white list," which can create management issues.

**User "helplessness"** A primary reason for helpdesk calls is that the user feels helpless in fighting spam and wants to act on improving accuracy by contacting the service provider. The call is usually triggered by an ineffective "Block Spam" button where the reported spam keeps reappearing; a bad reporting system is worse than no reporting system.

The presence of feedback buttons that actually work means users feel empowered to fix the problem for themselves and don't have to call support to report false positives and false negatives. The result is greatly improved customer satisfaction.

While the cost of customer dissatisfaction is difficult to quantify, churn and helpdesk costs account for double the cost of the infrastructure according to a report from Ferris Research, while subscriber re-acquisition costs can range from several hundred up to a couple of thousand dollars.

#### PHISHING AND VIRUS

Phishing and virus attacks directly affect the service provider's reputation. A phished user may blame the service provider for allowing the attack to happen, which can have a direct effect on churn.

Virus storms have been known to bring down a service provider's network. In the case of viruses, even a 1% increase in accuracy can make all the difference, since early detection can prevent a critical mass of virus-infected computers from developing.

#### THE CLOUDMARK ADVANTAGE

Cloudmark consistently delivers filtering accuracy in excess of 98%. In both live and controlled trials, Cloudmark's accuracy was proven to be 17 to 20% points higher than legacy systems. With Cloudmark, significantly lower volumes of spam, phishing, and virus attacks impact messaging infrastructures and subscriber inboxes.

In addition, Cloudmark's intelligent message fingerprinting is extremely light on resources. By using advanced fingerprinting algorithms, Cloudmark requires up to 90% less resources when compared to heuristics or rules-based techniques. This equates to proportional savings in MTAs and appliances.

Offering a positive user experience can be a key differentiator for service providers. The Cloudmark solution includes a number of capabilities that improve the user experience:

- Overall higher filtering accuracy and virtually zero false positives
- Feedback buttons (via the Cloudmark Network Feedback System) that actually work means users feel empowered to fix the spam problem without having to call support
- Subscriber solutions such as customized Webmail User Statistics, Cloudmark Secure Unsubscribe and Cloudmark Desktop enhance service value

For more information visit us at  
[www.cloudmark.com](http://www.cloudmark.com)

#### Headquarters

128 King Street, 2nd Floor  
San Francisco, CA 94107 USA  
Ph: +1.415.946-3800  
Fax: +1.415.946-3871

Cloudmark Europe Ltd.  
Garrick House  
26-27 Southampton Street  
London  
WC2E 7RS  
England  
Ph: +44 (0) 207-100-5224

Asia Pacific Office  
45/F The Lee Gardens  
33 Hysan Avenue  
Causeway Bay  
Hong Kong  
Ph: +852 3180 7768

Customer satisfaction and infrastructure impact are also driven by speed of response. While accuracy dramatically affects total cost, the speed of new threat detection is just as critical. For example, 100% virus blocking capability is useless if the blocking occurs a few days after outbreak.

Cloudmark blocks spam, phishing and virus mutations immediately with intelligent message fingerprinting. Once an attack has been fingerprinted, future variants are automatically stopped before they emerge. Defense against "new" attacks occur in real-time, without the need for manual research or analysis. Cloudmark's Global Threat Network is the world's largest threat detection network, consisting of over 120 million reporting sources, including service provider abuse teams, systems administrators, honeypots and ISP subscribers. This 24 x7 worldwide network is able to detect all forms of threats at the first occurrence of the outbreak.