

# **E-mail Integrity- Fundamental to Business Communications**



WWW

@

## Executive Summary

With e-mail being integral to the modern corporate communications ecosystem, effective handling of e-mail has never been more important than it is today. Some of the greatest benefits that would accrue from a more efficient e-mail management philosophy include:

- a) Lower costs in terms of resources and time expended in spam management, infrastructure downtime, and e-mail archiving
- b) Adherence to evolving compliance standards and protection from possible legal liabilities
- c) Business agility enabled by efficient and trusted communication

Whilst spam has inevitably emerged as a key area of concern for enterprises with respect to e-mails, they will do well to turn their attention to an increasingly significant issue, that of e-mail integrity. Indeed, there exist significant challenges for businesses in Asia in ensuring e-mail integrity due to low security awareness, proliferation of compromised endpoints, inability of spam engines to deal accurately with local language spam, and weak regulation. In light of this, the traditional notion of focusing on spam catch rates alone is no longer a sound decision-making criterion for the purchase of mail filtering products. Instead, the issue of false positive, where a legitimate e-mail gets flagged as a spam, is a serious issue for businesses due to the tangible and intangible costs associated with it. Thus, it is imperative for CIOs and IT managers to not only focus on solutions with high spam catch rate, but also look at solutions that can offer holistic e-mail integrity by combining high spam catch rate, low false positives, robust malware filtering, and data leakage prevention.

## I. Challenges Faced by Enterprises in E-mail Management

### I.1 The Growing Problem of E-mail Integrity

In the face of e-mail becoming a popular and effective tool for business communication, it has inevitably led to an onslaught of attacks and threats coming through the e-mail gateway. The sophisticated threat landscape has proved to be a bane to the private and public sectors that are increasingly dependent on e-mails for their day-to-day operations. This has, in turn, increased their exposure levels to external threats.

Some of the key challenges and threats that restrain e-mail from being an effective medium of corporate communication at present are spam, viruses, worms, spyware, malware, botnets, and phishing attacks launched through e-mails. More importantly, these threats are constantly evolving (see Figure I in the appendix).

### I.2 Cost of Spam

The rising criticality of e-mails in business communication, coupled with the increasing sophistication of threats coming from e-mails beyond mere spam, has meant that enterprises

can no longer regard spam as an inconvenience or a 'necessary evil'. In fact, Enterprises are beginning to count the cost of spam on their business profitability.

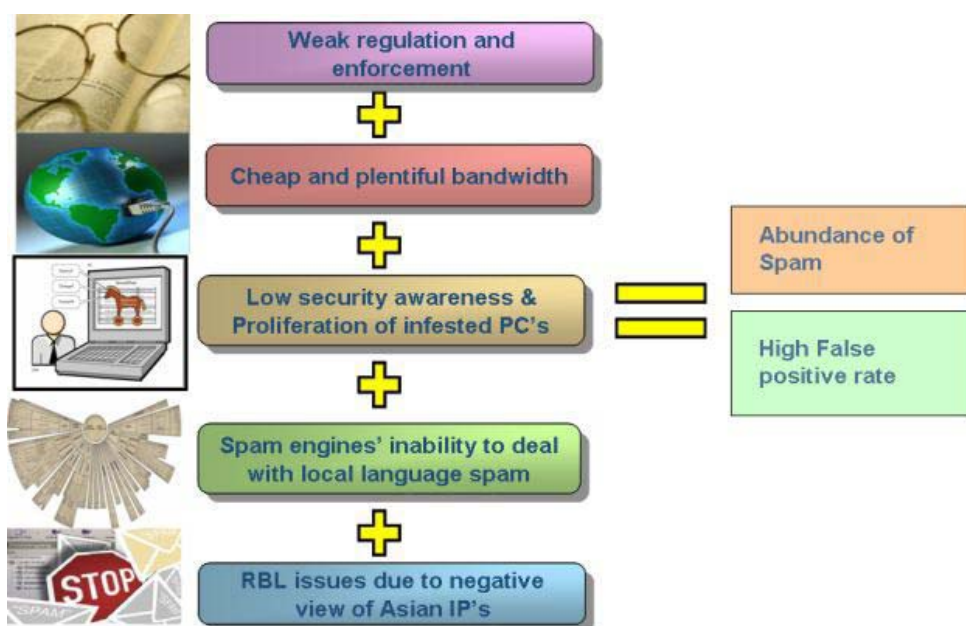
**Figure 2 : Cost of Spam**



### 1.3 E-mail Filtering Challenges

Spam is a global phenomenon, and companies in the Asia Pacific region are especially vulnerable, due to the large amount of spam originating from the region. This has caused severe mitigation challenges such as those shown in the chart:

**Figure 3: E-Mail Filtering Challenges in Asia Pacific**



















## 1.4 Spam Catch Rate, False Positives, and False Negatives

Indeed, with e-mail evolving to become an integral part of the corporate communications system, either in the initiation of business communication, the exchange of information, or negotiating agreements and scheduling meetings, there is a greater requirement to ensure that legitimate e-mails are being sent and received on an error-free basis. A single improperly classified legitimate e-mail can have more serious business and financial implications for an organization, compared to the potential costs that are attributed to spam. Consequently, it is important for the organizations at present to pay increasingly more attention toward the false positive rate.

To put the seriousness of false positives in perspective, we present a hypothetical inbox below containing legitimate messages, all of which can potentially be classified as spam by the reputation filters or directory-keyword based content filtering mechanisms commonly in use today (see Figure 4).

Figure 4. False Positive Rate Scenario

  <b>Jim Morrison</b>	» <b>Re://SUPER URGENT//ASSISTANCE REQUIRED TO CALCULATE ALL CHARGES</b>	<b>4:07am</b>
  <b>Cindy Lim</b>	» <b>RE: repair list for Feb</b>	<b>..:58am</b>
  <b>Defense e-security</b>	» <b>Innovative spam foxes Anti-Spam solutions</b>	<b>1:23am</b>
  <b>JetStar.com</b>	» <b>Print out your Jet Star Flight</b>	<b>12:26am</b>
  <b>OnlineTRADEmart</b>	» <b>LATEST STOCK POSITION</b>	<b>11:29pm</b>
  <b>Sys Admin</b>	» <b>Beware of phishing scams asking for passwords</b>	<b>Sep 28</b>
  <b>Rachel Schwarz</b>	» <b>Insurance Quotation for Tablette</b>	<b>Sep 28</b>
  <b>YX Huang</b>	» <b>FW: Direct fund transfer – LAST REMINDER!!!</b>	<b>Sep 28</b>

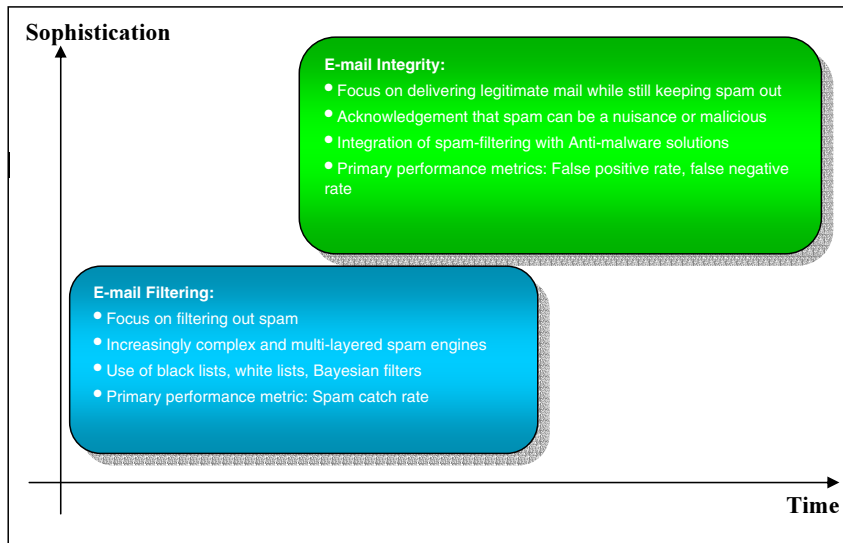
## 2 E-mail Filtering versus E-mail Integrity

Though the problem of spam is real as well as costly, the issue gives rise to two important, yet distinct, considerations:

- a) E-mail filtering
- b) E-mail integrity

Both issues lead to slightly differing approaches, depending on which of the two is given greater priority. E-mail filtering refers to effectively filtering out the messages that constitute spam, while e-mail integrity refers to ensuring that genuine e-mails are delivered to their destinations without mistakenly being filtered out as spam (see Figure 5)

Figure 5. Evolution of E-mail Security Perspectives



## 2.1 Dealing with Spam: One Issue, Two Approaches

By examining the mechanisms used to implement e-mail filtering and e-mail integrity, we can gain a deeper understanding of the key differences between the two philosophies and their impact on businesses.

### E-mail Filtering

Over the years, e-mail filtering has evolved to a stage where it is normal to expect commercial anti-spam solutions to have spam catch rates of over 95 percent. A high spam-catch rate is a point of parity in the anti-spam space, and is no longer a key differentiator of such solutions.

### E-mail Integrity

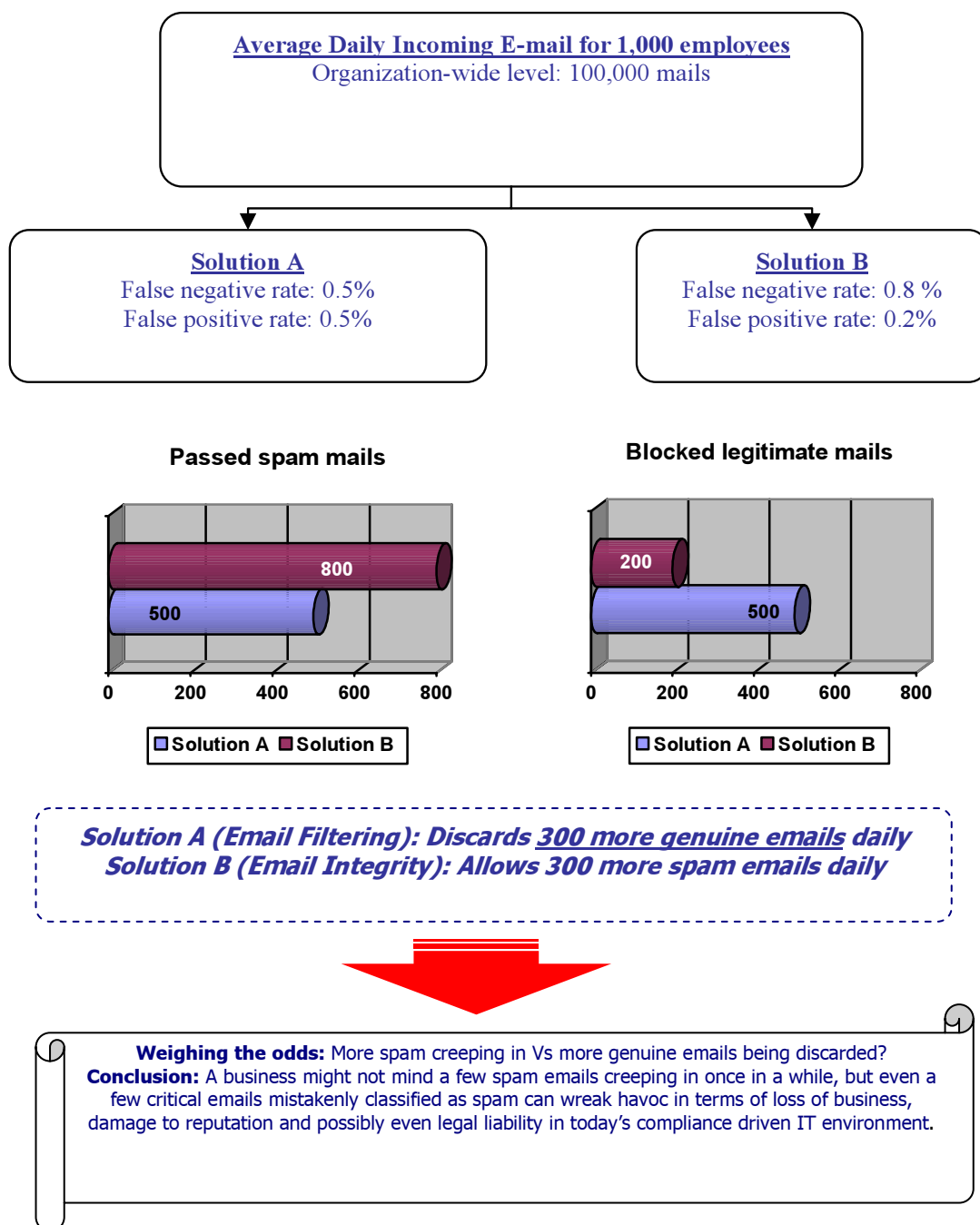
An alternate school of thought approaches the issue of spam from a different perspective. It begins with the premise that an e-mail must be first treated as genuine and then assessed as to whether it is spam. The reasoning behind this premise is that the priority of an e-mail delivery process should entail ensuring that a legitimate e-mail reaches its destination unhindered first, even before the filtering process to identify spam begins.

The idea of e-mail integrity is derived from the early implementations of mail delivery from trusted sources and the mechanics of establishing such trust. These mechanisms consisted of white-lists, which would identify and maintain a list of senders that a recipient would prefer to receive e-mails from. The best-of-breed current generation solutions make use of techniques such as sender identity services and history-based accept lists.

## 2.2 Weighing the Two Approaches

The ideal solution would catch 100 percent of spam with zero error rate of false positives and false negatives. Such solutions do not exist, yet companies are asked to strike a balance between the need for a high spam-catch rate and the importance of having a low false positive and negative rates (see Figure 6).

**Figure 6. Scenario within a Large Enterprise**



### 3. Conclusion

In today’s hyper-competitive environment, e-mails support many critical business functions inside the organization. Thus, it is critical for businesses to ensure e-mail integrity and protect legitimate e-mail traffic, without which the fundamental trust in business communications would be lost. Customers should look for a solution that combines the convenience of high spam catch rate with the benefits of a low false positive rate, which would help them realize the full potential of the rapidly evolving e-mail-centric communication infrastructure that underpins modern businesses. Thanks to advancements in technology, customers need not have a “trade-off” between false positives and false negatives anymore.

The customers are recommended to prefer solutions with very low false positive and false negative rates, which would serve them well in their quest for business competitiveness and high productivity.

### Appendix

Figure 1. The Evolution of Spam

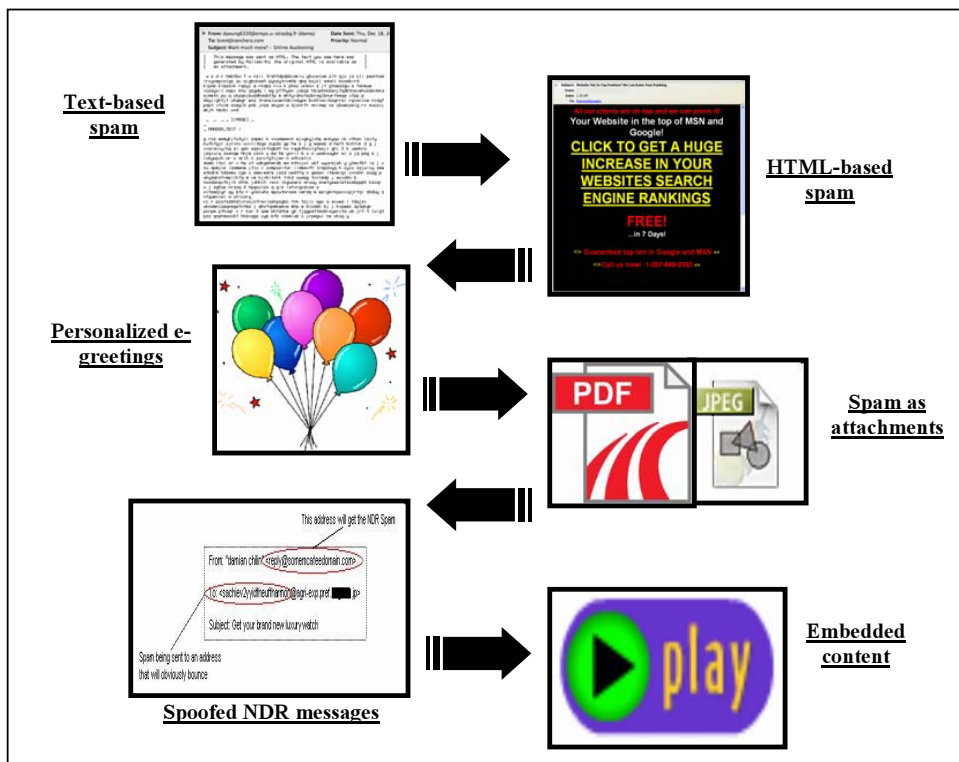


Table 1. Spam Metrics

Terminology	What does it Mean?
Spam Catch Rate	Percent of incoming spam that a solution identifies as spam
False Positive Rate	Percent of legitimate e-mails incorrectly classified as spam
False Negative Rate	Percent of spam messages that are passed through as legitimate mail

## Contact

Tel: (65) 6890 0999

Email: [apacfrost@frost.com](mailto:apacfrost@frost.com)

Website: [www.frost.com](http://www.frost.com)

## CONTACT US

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

São Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

### ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages over 45 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit <http://www.frost.com>.