

# ROI and Other Cost Benefits of Reputation-Based Services

Secure Computing® is a global leader in Enterprise Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.

## Table of Contents

Abstract .....	2
Introduction .....	2
Are You Really Out of Bandwidth .....	3
Mail Security Gateways – Buy What You Need Not What They Want You to Buy .....	4
Who Said Storage Was Cheap? .....	5
Malware Cleanup Cost Savings Due to Multi-Vector Reputation .....	5
Overall Cost Savings .....	6
Conclusion .....	7

### Secure Computing Corporation

**Corporate Headquarters**  
55 Almaden Blvd., 5th Floor  
San Jose, CA 95113 USA  
Tel +1.800.379.4944  
Tel +1.408.494.2020  
Fax +1.408.494.6508

**European Headquarters**  
Berkshire, UK  
Tel +44.(0).1344.312.600

**Asia/Pac Headquarters**  
Wan Chai, Hong Kong  
Tel +852.2598.9280

**Japan Headquarters**  
Tokyo, Japan  
Tel +81.3.5339.6310

For a complete listing of all our global offices,  
see [www.securecomputing.com/goto/globaloffices](http://www.securecomputing.com/goto/globaloffices)

Given that spam can comprise as much as 95 percent of all email, an appliance that eliminates even half of that stream relieves pressure on spam filters, mail servers, and anti-spam services. That translates into less hardware, less traffic, and big savings.

– InfoWorld  
[http://www.infoworld.com/article/05/08/29/350Peditor\\_1.html](http://www.infoworld.com/article/05/08/29/350Peditor_1.html)

## Abstract

In simplest terms, deploying a reputation service at the network edge is analogous to having a peephole in the front door of your house. You let in people you know and trust, question the ones you don't know, and shun the ones who look suspicious. Just by taking these simple measures you reduce your risk. Similarly, organizations can save a lot of money by filtering the bad traffic at the edge of the network using reputation based services. Among other things, companies can save considerable amounts of money by:

- Improving bandwidth with fewer expenses
- Reducing infrastructure expenses to process already filtered content
- Savings in the form of lesser storage
- Eliminating the need to archive spam messages for compliance purposes
- Protecting against phishing, zombies, spam, malware, viruses, etc. and subsequent cleanup costs

After examining this document, the reader will not only understand the importance of securing the network edge with a global reputation service but will also appreciate the huge savings that can be realized. Furthermore, the paper explains how the Secure Computing® TrustedSource™ technology reputation system adds a critical extra layer of proactive, advanced protection to help organizations accurately detect and block all types of threats to their messaging, Web, and network environments.

## Introduction

An organization's network is the backbone of its very existence and is critical to its day-to-day success. Protecting the network is protecting the organization itself. Today there are even more threats to the network, from all sides and all corners of the globe:

- Email and other messaging protocol attacks including spam, Phishing, directory harvest, and denial of service
- Web-based attacks such as malware-infected URLs, unfiltered SSL encrypted traffic, and viruses
- Network attacks that take advantage of system-level vulnerabilities
- Blended threats that combine multiple attack vectors

New, advanced functionality built into today's Internet (Web 2.0) has made these types of attacks easier than ever and attacks that were once limited to the messaging layer can now penetrate the enterprise through the Web and network layers as well.

Yesterday's security technology does not adequately fulfill the needs of the Web 2.0 world. The signature-based approach is no longer effective because threats are evolving and morphing faster than ever. One enterprise by itself often doesn't have access to enough information to be able to identify and act on threats quickly enough to render them harmless. As a result, modern gateway security must incorporate several characteristics—most importantly, the proactive anticipation of threats, so that they can be caught *before* they cause damage, not after.

Secure Computing TrustedSource global reputation system bridges the worlds of messaging, Web, and network security, creating an umbrella of multi-platform protection that has long been absent from Internet security. Like a virtual credit agency, TrustedSource assigns a reputation score and further classifies senders as good, bad or suspicious based on an in-depth analysis by processing hundreds of attributes of each sender and each message.

By combining years of industry-leading research with the unmatched capabilities of spam profiling, Secure Computing has made ground-breaking discoveries. TrustedSource analyzes hundreds of billions of messages/transactions per month from Secure Computing's global enterprise network of sensors

located in enterprises and government institutions. Sender reputation scores in TrustedSource are based on sender history, message characteristics and URL characteristics. It assigns reputation to the following entities:

- IP senders
- Messages
- Domains
- URLs
- Images

Secure Computing appliances worldwide report back to TrustedSource, giving it a real-time view of virtually all commercial traffic on the Internet. Any deviations from normal sending patterns are picked up by TrustedSource and reputation scores are dynamically updated. Those reputation scores are immediately available to all appliances in the field leveraging the intelligence of TrustedSource.

Let us revisit the analogy that we mentioned in the abstract; Reputation service on network edge is similar to the peephole on your front door (Figure 1).

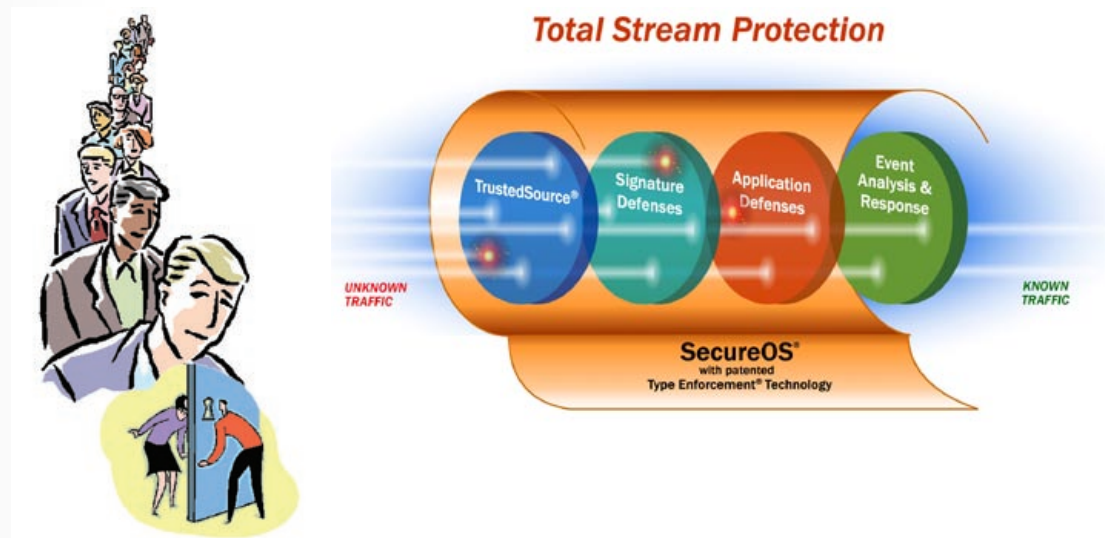


Figure 1: Analogy between peephole and reputation service on network edge

Imagine how many couches you would need in your living room if you invited every single person in who knocked at your door or was just passing by. Not deploying a reputation service on the network edge is the networking equivalent. Every single year there is a huge surge in spam emails especially towards the beginning of the holiday season. In 2007, according to Secure Computing Research, spam reached 94% of total email volume. If we go by IDC's report—"Worldwide Email Usage 2007-2011 Forecast: Resurgence of Spam Takes Its Toll" that would mean 94% of 10.49 trillion worldwide email messages are spam, a total of 9.86 trillion messages. Let us now look into the details of where and how organizations save money by using reputation based services on the network edge. The default global parameters below are collected from representative samples of thousands of enterprise networks utilizing TrustedSource intelligence in their email infrastructures. You can adjust these parameters and customize them to match your own data.

## Are You Really Out of Bandwidth?

Inbound email is doubling in volume every six to eight months for organizations, mostly because of spam. This is forcing IT to add additional bandwidth, mail security gateways and mail servers to their infrastructure. But adding new infrastructure every 6-8 months is not an option for most organizations. The truth is that organizations are actually not running out of bandwidth but spending their resources on messages that can be filtered at the network edge without having to examine the payload at all. In the absence of a global reputation service the mail server has no choice but to accept the connection and examine every piece of mail it contains. This wastes a lot of otherwise useful bandwidth and processing time on critical email servers. It also causes a delay of good emails into inboxes throughout the company.

Several studies have shown that a single organization can waste several gigabytes of bandwidth receiving unwanted spam emails and unfortunately is liable to pay for this. Even if the cost of bandwidth is not much by itself it certainly contributes towards the overall cost of spam. Let us consider an organization of roughly around 1000 employees.

Average cost of Internet connectivity per month	= \$5,000
Bandwidth used by email	= 50%
Average percentage of email that is spam	= 90%
Average % of spam dropped at network edge using TrustedSource	= 60%
Annual cost of bandwidth used by spam if not filtered at edge	= \$5,000*0.50*0.90*0.60*12
	= \$16,200

So, this is the amount of money that a company saves by blocking spam using reputation service at the network edge.

## Mail Security Gateways – Buy What You Need not What They Want You to Buy

With the recent surge in spam security officers are being forced to believe that they need to upgrade their mail security solution by adding more hardware. Whereas, the truth is that most of the bad stuff can be filtered even before it reaches the mail servers. Though the throughput of different anti-spam solutions varies depending on size of appliance, anti-virus scanning, etc. on average we can assume a decent sized appliance can filter somewhere around 50,000 emails per hour at the peak rate. The prices of these solutions also vary a lot but let us assume an average price of \$5,000 for the performance mentioned here.

A recent blog (<http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html>) talks about the future of spam and says that now spammers can buy managed servers running thousands of zombies which are capable of sending 7,000 emails per second. This was an advertisement that was published by a Russian company selling these servers. The average cost of these servers was in the range of \$3,000-\$4,000.

As these managed spamming servers sound very affordable and have a lot of value, they can easily get a contract from thousands of spamming companies. Let us assume, they use one of these servers on behalf of 3,600 companies and send out 7,000 emails per second per company. One of the very basic spam attacks consists of harvesting one email address per organization and then guessing the most common first and last names and shooting tons of emails to these emails addresses. To be very conservative let us assume an organization gets attacked only once a year with such an attack. Let us do some scary math here to calculate the cost involved (as good email will be equivalent to rounding error here, we are ignoring that number).

### In absence of reputation-based service:

Total emails received per hour: 7,000 (per second) \* 60 \* 60 = 25.2M emails  
 Average capacity of one mail security appliance: 50,000 emails per hour  
 Number of Appliances needed: 25.2M/50,000 = 504 appliances  
 Cost of 504 appliances (Average cost per appliance \$5,000): \$2.52M

### In presence of reputation-based service:

Total emails received per hour: 7000 \* 60 \* 60 = 25.2M emails  
 Emails filtered at Network edge using TrustedSource: 60% of all email = 60% of 25.2 M = 15.1M  
 Emails going to the mail security appliance: 25.2M – 15.1M = 10.1M  
 Average capacity of one mail security appliance: 50,000 emails per hour  
 Number of Appliances needed: 15.1M/50,000 = 302 appliances  
 Cost of 302 appliances (Average cost per appliance \$5,000): \$1.51M

**Savings because of TrustedSource = \$2.52M -\$1.51M = \$1.01M**  
**= 40% in savings**

One thing to be understood here is that an organization would need these many appliances in case they choose to be up and running even under such a massive attack. This would be the case with organizations for which email is mission critical and email downtime would mean direct loss of business. And unfortunately this is the case with almost every single organization around the world.

## Who Said Storage Was Cheap?

There are myriads of state, industry and national regulations, especially Sarbanes-Oxley Act and HIPAA, which include provisions to retain all modes of electronic communication for years. These regulations make storage costs a key factor for organizations that are required to save all of their email. The critical loophole to note here is that any email that actually arrives at the email server must be archived; those that get dropped **before** the email server don't.

The average size of spam has more than doubled because of the new spamming techniques including image spam. The reason for including images is sometimes to make the email look attractive and at other times to obfuscate the text to foil the intelligence of anti-spam solutions. Whatever the reason for using images or attachments is, the impact is huge on the overall storage and bandwidth capabilities due to the sheer volume of spam floating around. Moreover, with ever changing spam techniques leaning more towards using different file formats like PDF, MP3, video the future does not look very bright. According to Secure Computing research the current average size of spam with attachments is 20KB. Companies that do not block spam at the perimeter usually meet with a storage crunch as these bloated spam messages often get archived along with legitimate business email.

Let us now calculate the cost of storage associated with spam for an organization of 1,000 users.

Connections per user per day	= 117
Total number of connections daily	= 117,000
Average # of messages per connection	= 1.3
Total number of messages daily	= 152,100
Average percentage of email that is spam	= 90%
Average number of spam messages daily	= 136,890
Average % of spam dropped at network edge using TrustedSource	= 60%
Average number of spam messages blocked daily	= 82,134
Average size of spam message with attachments	= 20 KB
Total size of spam blocked daily	= 20 KB * 82,134
	= 1,642.7 MB
Average cost of storage/MB	= \$0.50
Total money wasted in storing spam daily	= \$0.50 * 1,642.7
	= \$821
Total money wasted yearly	= \$821 * 365
	= \$300,000 (approx)

*(We intentionally used 365 days and not 260 business days in a year because we get spam every single day of the year, usually more on weekends)*

This is the case taking average spam size as 20 KB; imagine what would happen if MP3 spam becomes successful whose average size would be 2MB (100 times more). This \$300,000 figure will get extremely horrifying and would convert to a waste of \$30 million every single year because of absence of reputation service at network edge.

## Malware Cleanup Cost Savings Due to Multi-Vector Reputation

Costs can soar to clean up from attacks launched by multiple vectors, also known as blended threats. Unlike other reputation services, TrustedSource provides reputations for not only IP addresses but also domains, URLs, images and messages. This allows TrustedSource, uniquely, to cross reference multiple reputations together to form accurate analysis of threats as they are happening. Quite recently spammers have started using legitimate links in their spam emails for taking the user to the malicious/

Organizations spend up to \$13 billion globally for direct malware remediation costs

– TechNews World  
<http://www.technewsworld.com/story/59579.html>

spamming Web sites. These legitimate URLs can be for Google (exploiting “I’m feeling lucky” feature <http://www.google.com/search?q=independent+telemarketers&btnI=ec>), Wikipedia ([http://www.toptechnews.com/story.xhtml?story\\_id=101003HCTOK6](http://www.toptechnews.com/story.xhtml?story_id=101003HCTOK6)), Telegraph (Figure 2), YouTube (Storm Worm), etc.



Figure 2: Legit URLs being misused in spamming

Most, if not all, of the anti-spam solutions use a URL blacklist to filter malicious/spam URLs. Unless specifically asked to, no anti-spam solution in the world would block a Google, Wikipedia or a Telegraph link. If any of these spam emails happen to be coming from a newly created bot (hence no reputation available), most reputation services would not block them and they would end up in your inbox. Fortunately, TrustedSource would block such emails based on either of these two things:

1. Message reputation
2. Reputation input from web security product Webwasher® identifying that destination URL contains Malware

Forrester surveyed 153 IT and security professionals about security technologies in their organizations. The organizations surveyed included enterprises with 1,000 employees or more. Roughly around 50% of the organizations agreed to have paid \$25,000 in Malware cleanup costs the previous year. Thus, for the calculation sake it would be safe to assume:

Malware cleanup cost per year for an organization of 1000 employees = \$25,000

Again, Malware cleanup cost is just one aspect of the savings that come from protection from blended threats. Other costs include losses due to Phishing, purchase of spam products, data leakage, reputation loss, regulatory penalties, etc. But we will avoid them here for the simplicity of the discussion.

## Overall Cost Savings

What we saw in the previous sections is just the tip of the iceberg and there are many other benefits of having reputation service at the network edge. We were consistent in all our examples and considered an organization of only 1,000 employees. The default global parameters used were collected from representative samples of thousands of enterprise networks from around the globe utilizing TrustedSource intelligence in their email infrastructures. Let us now try to summarize the results.

Organization size	= 1000 employees
Timeframe	= 1 Year
Bandwidth savings	= \$16,200
Infrastructure savings	= \$1,010,000
Storage savings	= \$300,000
Malware cleanup cost savings	= \$25,000
<b>Total</b>	<b>= \$1,351,200</b>

So, the total savings year after year is in the range of 1.36 Million USD. One would assume an appliance running TrustedSource and offering these huge amounts of savings every year should cost at least a few hundred thousand dollars. Fortunately, this is not true. TrustedSource can be deployed in various forms

(Figure 3) and the price tag starts at less than \$10,000 USD for an organization of 1,000 users. With this cost and savings ratio the breakeven time frame in number of days would be:

$$\begin{aligned}
 \text{Breakeven in number of days} &= \frac{\text{Cost}}{\text{Savings per day}} \\
 &= \frac{10,000}{(1,351,200/365)} \\
 &< \mathbf{3 \text{ Days}}
 \end{aligned}$$

*Note: To be consistent with earlier calculations we have again used 365 days in a year and not just working days owing to the fact that we get spam all year round. If we use 260 days instead the break even number of days would reduce to less than 2 days*

Sounds impossible, but is indeed true. An organization investing in TrustedSource would break even in less than 3 days in the form of savings.

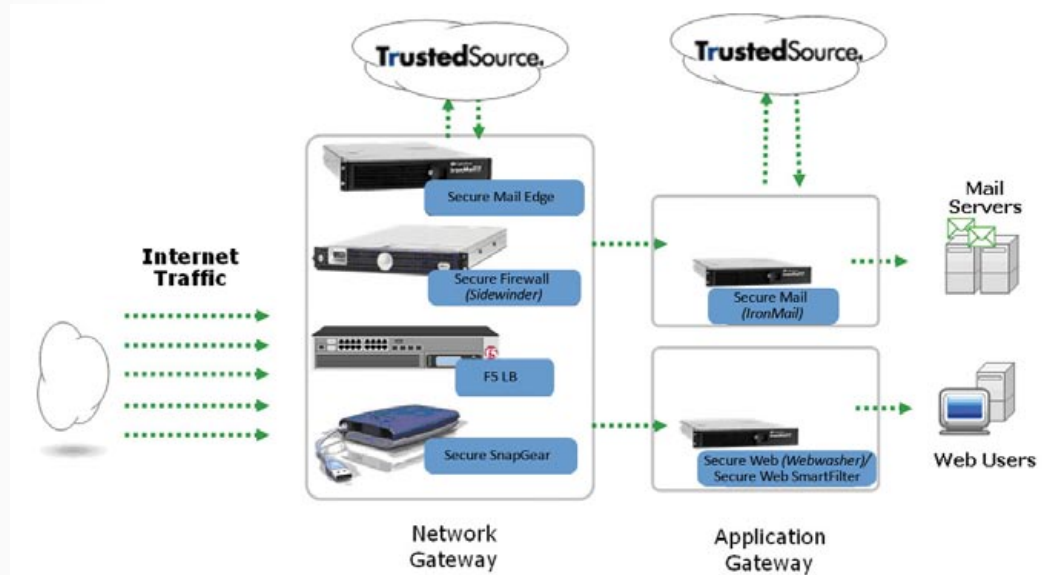


Figure 3: Deployment options of TrustedSource

## Conclusion

In this paper we made the reader aware of the huge costs savings involved in having a reputation service at the network edge. These savings came in varied forms:

- Reduced bandwidth requirements
- Infrastructure savings
- Reduced storage costs
- Reduced malware cleanup costs

We also talked about the unmatched protection offered by TrustedSource and costs involved with it. It was shown that the ROI was huge and the cost was recovered in the form of savings in less than 3 days. Deployment of TrustedSource is very flexible and can be deployed in any new or existing network within minutes. If network is the backbone of any organization and email its heart, TrustedSource is the shield that protects these from known and unknown threats without which even a smallest of the worms can paralyze the functioning of the whole organization.