

# **AN EVALUATION OF THE TOTAL COST OF OWNERSHIP OF E-MAIL SECURITY SOLUTIONS**

*A Frost & Sullivan White Paper*

This white paper explores the differences between service and product models for e-mail security. Readers will learn about the various considerations for implementing e-mail security in each of these two formats through an analysis of the total cost of ownership (TCO) of each deployment option. Ultimately, this paper aims to improve the reader's ability to make informed and accurate purchasing decisions by uncovering the costs of products and services that are seldom considered before a purchase is made.

ABOUT  
FROST &  
SULLIVAN

## **ABOUT FROST & SULLIVAN**

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the information technology industries/industry. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for noncommercial individual reference or private use within your/an organisation, and thereafter it may not be re-copied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialise or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write to:

Frost & Sullivan  
2400 Geng Road, Suite 201  
Palo Alto, CA 94303-3331, United States

## EXECUTIVE SUMMARY

The burdens that spam and malicious code have created for organisations are both critical and obvious. The costs of spam can be associated with lost productivity, as well as additional infrastructure resources required to forward an ever-increasing number of messages. What is less obvious is the cost associated with e-mail security solutions. To date, three categories of e-mail security solutions have emerged in the form of e-mail security software, e-mail security appliances and e-mail security services.

Frost & Sullivan took a deeper look at the costs associated with each of these solutions and built TCO models to compare the true costs of the solutions over their lifetime of use. Variables such as purchase price, platform installation, network integration, configuration and monitoring were analysed to calculate the TCO for e-mail security solutions in both large and small network environments.

The first TCO evaluation compares the cost of the Postini e-mail security service with the cost of integrating an e-mail security appliance in an environment of 300 users. While the costs of each solution were similar, the Postini service would cost approximately 12 percent less than a comparable appliance solution.

The second TCO evaluation compares the cost of integrating the Postini e-mail security solution with the cost of an e-mail security software solution in a large environment of 10,000 users. This evaluation proved that the Postini solution was over 32 percent less expensive than a comparable software solution.

Additional advantages such as integrated antivirus filtering, e-mail spooling and the external filtering of spam and viruses create even more un-quantifiable value. These features offer increased protection, disaster recovery capabilities and reduce the amount of bandwidth and network infrastructure equipment required for Postini customers.

The results prove that by leveraging a services model, customers are not only able to save money on the total cost of ownership of an e-mail security solution, but are able to increase security and scale their deployments more linearly than by purchasing software or appliance solutions that are installed at the customer location.

## TABLE OF CONTENTS

About Frost & Sullivan	2
Executive Summary	3
Introduction	5
The Models	5
The E-mail Security Problem	5
Appliance-based Solutions	6
Software Solutions	6
Service-based Solutions	6
TCO - The Real Equation	6
How TCO Varies from Purchase Price	6
TCO Factors	7
Planning	7
Purchase Price	7
Procurement	7
Platform Installation	7
Integration	8
Configuration	8
Monitoring	8
Upgrading	9
Patching	9
End of Life	9
Step Function	9
Hypothetical Cost Evaluation	10
Small Environment Cost	11
TCO Variables and Considerations	11
"Competitor A" Total Cost of Ownership	11
Postini Total Cost of Ownership	12
Large Environment Cost	12
TCO Variables and Considerations	12
"Competitor B" Total Cost of Ownership	13
Postini Total Cost of Ownership	13
Conclusions	15

## INTRODUCTION

### The Models

#### The E-mail Security Problem

E-mail has become one of the most widely used communication mediums in the world. Like the rest of the Internet, it is the very ubiquity of this medium that limits the security of the system. Traditional threats against e-mail users and systems include traditional viruses, Trojans/trojans and worms (collectively referred to as malware). However, a newer threat has emerged in the form of spam. Unsolicited e-mail has been measured as representing 60-80 percent of all e-mail communication. For many, spam is merely a nuisance, but taking a deeper look at this nuisance reveals some definitive security risks and business costs.

One of the most obvious costs of spam is the cost of the additional bandwidth and network infrastructure resources (servers, routers, etc.) associated with large amounts of spam. Another cost centres around the decreased productivity of a workforce that is constantly combing through and/or reading junk e-mail. Since many spam e-mails are solicitations for pornographic web sites, offensive material can create undesirable work conditions and even corporate liabilities for not preventing such material from reaching employees. Widely recognised statistics estimate the business cost of transmitting, storing, reading, and ultimately deleting a single spam e-mail to be approximately £0.55 per spam message. Taking this into account, many anti-spam e-mail security solutions are able to pay for themselves within one month.

Beyond the increased costs, certain security risks can be introduced through e-mail and spam as well. In addition to the well-known malware that can be propagated through spam, phishing scams can be introduced to users through spam e-mail. These phishing scams use e-mail to impersonate legitimate communications from businesses to users. The e-mail will request the user to click on a link contained in it in order to log into their account. However, the link actually brings up an illegitimate representation of a business' web logon page. When the user enters their logon credentials, the information is captured and stolen to be used for nefarious purposes.

Since these risks have begun to pose heightened security risks/threats and have also increased costs to/for administrators, many solutions have been developed to combat them. E-mail security solutions vary in capability and integration strategy, but can logically be classified into three groups, namely services, software and appliances.

## Appliance-based Solutions

Today, many security technologies are sold as appliance-based solutions. These products are pre-loaded with software applications and operating systems to provide an out-of-the-box experience for users. Appliance-based solutions have become the de facto standard for many security technologies, including firewall, IPSec/SSL VPN, and intrusion detection and prevention systems because of the performance requirements of security solutions. Additionally, an appliance-based solution is usually hardened by removing unneeded services. This hardening improves performance and increases the security of the device. Examples of appliance-based e-mail security solutions include Borderware's MXtreme and Barracuda's Spam Firewall.

## Software Solutions

Software solutions can be purchased independent of an existing appliance. In this implementation option, the customer supplies the server, which the software runs on. This server could be a new, dedicated or high-performance server, or may be the existing mail server within an organisation. Examples of e-mail security software solutions include Symantec's Brightmail Anti-Spam and NetIQ's MailMarshal.

## Service-based Solutions

Service-based solutions are not implemented within the customer's network. Rather, all e-mail traffic destined to the customer's network is routed through the service provider's equipment where scanning and filtering take place. Subsequently, the scanned e-mail traffic is forwarded to the customer for delivery, or blocked according to the customer's security policy. Examples of service-based e-mail security solutions include Postini and MessageLabs.

## **TCO - THE REAL EQUATION**

### **How TCO Varies from Purchase Price**

Administrators often perform initial ROI analyses on products by comparing the cost of the product or service to the cost or risk that the threat creates. However, in order to accurately gauge this cost difference, the system needs to be practically evaluated to understand the cost of using and maintaining it, in addition to the cost of the system itself. Total cost of ownership (TCO) is the quantification of the costs associated with the installation, configuration, management, and maintenance of a system in addition to the initial cost of purchasing the system. The following section investigates the hidden costs that can be associated with installing an e-mail security solution.

**TCO - THE REAL  
EQUATION**

## TCO Factors

### *Planning*

Planning costs are invoked before the purchase of a solution is actually made. These costs can vary greatly depending on the size and scope of the organisation, as well as the size and scope of the solution being implemented. Implementing a solution to a single LAN with a limited number of users requires less planning than deploying the solution to multiple offices in complex networking environments with multiple e-mail servers. Planning requires a review of the existing corporate security policies to understand how a solution will fit in with and modify the existing security policy. A list of required products or services to be purchased should also be made at this point.

Additional planning items include the notation of how and when the solution will be delivered to multiple offices, how administrators will integrate the solution, and who will be responsible for these tasks. More complicated solutions will require more planning time to ensure that the rest of the purchase and implementation process goes smoothly.

### *Purchase Price*

The purchase price of an e-mail security solution can include the price of an appliance (in the case of a product purchase) as well as the associated licensing fees. These licensing fees are fairly straightforward and are easily quantifiable, and include not only the license for the use of the solution, but also the costs of any subscription-based threat pattern updates, extended warranty, and technical support or features that accompany the e-mail security product or service.

### *Procurement*

Procurement costs can vary depending on the purchasing habits and procedures that an organisation has in place. These costs are associated with the time taken to contact a seller (whether that seller is a vendor selling solutions directly or a reseller), to negotiate a purchase price, and place an order. If a solution is not instantly available, there may be additional wait time required before the solution is delivered to the purchaser. These costs can also include the time associated with a purchase approval process. Procurement expenses can be exacerbated if the e-mail security solution is being implemented in geographically disparate offices. Generally speaking, these costs are minimal and are associated with the purchase of all solutions.

### *Platform Installation*

For e-mail security products that are sold as appliances, the cost of the hardware platform is added into the purchase price. However, many solutions today are offered as software-only solutions, which require the procurement and purchase of a separate hardware platform for the software to run on. Planning costs are extended here, as administrators must decide on acceptable performance and throughput requirements, which can complicate the hardware decision. Platform costs can also increase procurement costs, in the frequent case that a different vendor or reseller must be invoked to purchase the hardware from.

Additional platform costs surround the installation of the software on the hardware device. This process is complicated by the need to transform the device from a multipurpose server to a hardened, secure infrastructure component. The process of hardening involves removing all services that are not necessary to perform the specific, limited tasks assigned to the e-mail-filtering device. The removal of these additional services protects against the vulnerabilities and exploitation of these unneeded services. While there are many documented references to best practices for hardening servers, the task can be a daunting one for unqualified security administrators, and a time-consuming task even for qualified professionals.

#### *Integration*

Integration costs can be associated with both a service and a product, and refer to the physical installation of a device into the network infrastructure, or the configuration of a service to be provided to the network. This integration can demand the changing of settings, the redirection of traffic flow (Message Transfer Agent and Mail Exchange Record adjustment), and the modification of infrastructure components to make the system work properly. Many smaller IT departments will often hire a consultant to advise on the proper procedures for making these changes, to ensure against misconfigurations that may otherwise result in system failure.

In the event that e-mail security software is intended to run on the customer's existing mail servers, it must be compatible with the other services running on the device, including antivirus and calendaring functions. More importantly, the software must be manually configured to perform its function in coordination with the functions already running on the server.

#### *Configuration*

Configuration tasks pertain to adjustments that must be made after the solution is initially integrated into the network. Once the solution has been implemented, numerous configurations regarding the sensitivity of filters and the types of spam to block must be made. Additional configurations provide instructions on how to treat suspicious e-mail, whether to block, quarantine, delete, or store. Storage parameters must be established to determine the length of time spam will be stored and a maximum allowable storage allocation size. When considering the need to make each of these configurations for each user, the configuration task can become complex and time-consuming since various users will have differing policies that they wish to enforce to avoid false positives and false negatives. If these policies are implemented in a less than ideal fashion, users will protest, flooding the help desk with calls and complaints about the solution.

#### *Monitoring*

After the initial installation and configuration tasks are complete, administrators must continually monitor the solution to ensure accuracy and efficacy of the solution. Performance checks ensuring acceptable throughput and delay are used to verify that the solution is working optimally. This task is an ongoing activity that is accomplished throughout the duration of the solution's existence. When less than ideal conditions are experienced, configuration adjustments are made during this phase.

### *Upgrading*

As product vendors continually strive to improve their solutions, upgrades will become available. These upgrades are occasionally offered free of charge, but major product upgrades that occur, approximately, annually are generally charged for. The continual investment in product improvements must be accounted for and budgetary requirements met in order to procure these upgrades. While these upgrades usually bring significant improvements to the product solution, they can often create interoperability and configuration challenges upon implementation. Moreover, the purchase and the installation of these upgrades brings the user back to the first TCO factor and make it necessary for the purchaser to complete the entire process again. Advantages of the service model allow the service provider to shoulder the burden of implementing these changes, which are generally seamless to the customer.

### *Patching*

As network administrators in today's IT departments are aware, patching has become a regular solution to the continually evolving vulnerabilities that are being discovered in networking equipment. Adding to the complexity of patching requirements is the need to track which patches are important enough to implement, along with the increasingly important task of testing the patch before implementing it into the networked environment. Without testing, patches face the same disadvantages as upgrades, potentially causing interoperability or configuration issues. Again, the service model provides advantages in that the patching tasks are handled by the service provider (SP), alleviating this concern for administrators.

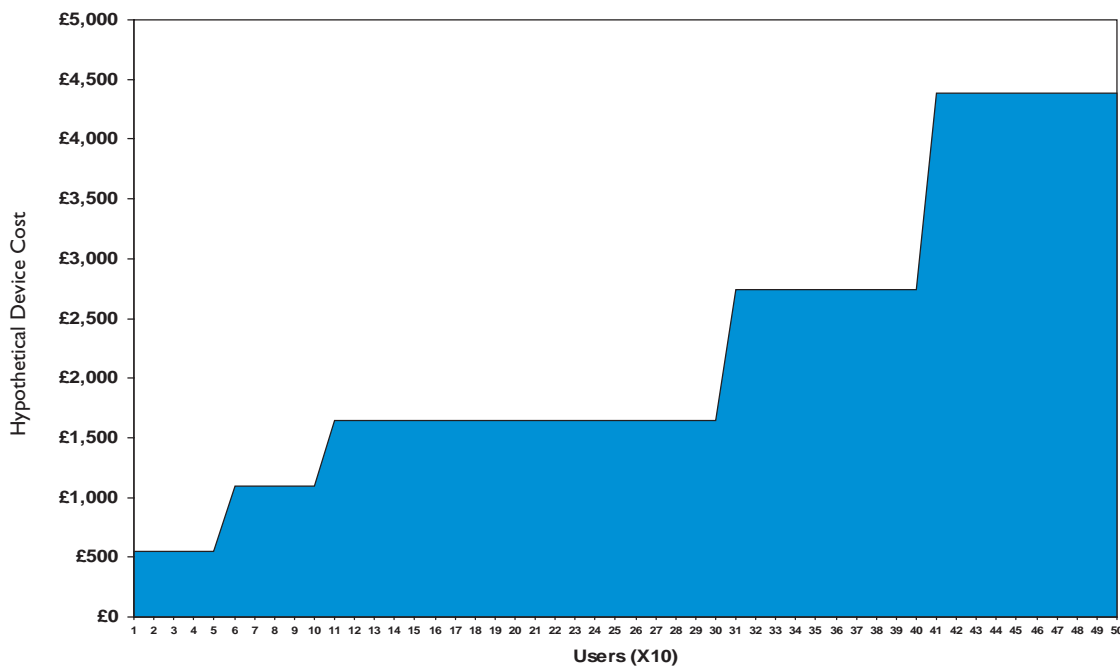
### *End of Life*

Eventually, the e-mail security software, the hardware, or both must be replaced. Major software upgrades require a complete reinstallation of the solution, and hardware performance capabilities will eventually need to be updated with new platforms. When either or both of these core components of the e-mail security solution must be replaced, the entire TCO list must be revisited to revamp the solution.

### *Step Function*

The Step Function refers to a seldom-considered task that administrators often discover by surprise only after a solution has received significant investment. The concept points to the maximum sustainable number of users that any hardware/software combination can support. Whether the solution is purchased as a bundled appliance or as a separate software and hardware solution, administrators will be limited to a certain number of users that the product can support. If the number of users on a network grows past the maximum sustainable number of users, a completely new hardware platform or appliance must be deployed to support these new users. Even if the organisation only needs to add a few new users, the entire TCO matrix must begin anew to implement higher performing hardware to support these additional users. This is referred to as the "Step Function" because even one new user requires the organisation to step-up to a higher performing device as illustrated in Chart 1. This forces potential purchasers into the difficult position of having to accurately predict the growth of the number of users, and having to change their cost structure per user for each prognostication.

Chart 1: The Step Function



Source: Frost & Sullivan

Additional consideration can be given to the amount of underutilisation that occurs when an organisation does not use the product to support the number of users that the product is capable of supporting. Here, resources are wasted by purchasing more than are needed or utilised. Conversely, a service-based per user model allows users to be added and removed as needed, so that an organisation is never paying more than it needs to, and is never faced with the expensive task of revamping its solution to support more users than the solution allows.

### Hypothetical Cost Evaluation

In this section of the paper, Frost & Sullivan has illustrated a hypothetical cost evaluation of various competitive solutions along with the Postini-managed service solution. Because implementation tasks and costs vary considerably between large and small network environments, Frost & Sullivan has provided this analysis for a small environment (300 users) and a large environment (10,000 users). In each of the TCO analyses, Frost & Sullivan has accounted for the number of hours required to perform each previously noted TCO task, and the purchase prices associated with products, subscription services, licensing and hardware. All these models assume an hourly salary rate of £39.81 for a network administrator. Monetary figures have been rounded to the nearest whole pound sterling.

Throughout these analyses, Frost & Sullivan has created estimates using the list prices of equipment and services because the variations in the types of discounts that different customers are able to receive differ greatly.

In an effort to make an accurate comparison between the feature sets of the Postini service and competitive products, each TCO analysis will consider deployments made in a high availability, fault-tolerant configuration. This is the recommended configuration of anti-spam solutions, because if an anti-spam device fails, the previously mentioned £0.55 per spam cost will quickly ramp up to equal the high availability option cost. In such an event, a single day without an anti-spam solution rivals the cost of most fault-tolerant configuration options. Further, failure of the anti-spam solution may bottleneck or block all e-mail delivery, creating an unacceptable situation.

Research in the firewall/IPSec VPN market has proven that the average lifecycle of a firewall is approximately three years. Therefore, this paper will analyse the costs associated with an e-mail security solution over a three-year period.

**Small Environment Cost**

*TCO Variables and Considerations*

Irrefutably, the amount of time required to plan, implement, and manage an e-mail security solution in a small environment is less than in a large, geographically disparate environment. For this small environment analysis, Frost & Sullivan has compared the integration of an e-mail security appliance with the cost of the Postini service.

An estimated number of hours is listed for each of the TCO variables discussed previously. The small environment analysis will assume a total of 300 mailboxes on a single site, with a fault-tolerant, high-availability e-mail security solution. Also included in the figures are the tangible list costs of hardware and associated annual services that would be paid to an e-mail security appliance vendor, or the per user licensing and activation fees that would be paid to Postini.

*"Competitor A" - Total Cost of Ownership*

Figure I below details provides the TCO of using an e-mail security appliance in a small network environment. Because appliances arrive with software pre-installed, there are no costs associated with platform installation.

Figure I : "Competitor A" - Total Cost of Ownership for a Small Environment

TCO Factor	Activities/Details	Hours Year 1	Hours Year 2	Hours Year 3	Purchase Price Year 1	Purchase Price Year 2	Purchase Price Year 3
Planning	Review available options/features	16.0					
	Perform TCO analysis	3.0					
	Delegate responsibilities	1.0					
	Modify security policy	2.0					
Purchase	Appliances				£3,998		
	Signature/rule updates				£645	£645	£645
	Replacement insurance				£645	£645	£645
Procurement	Distributor/vendor contact	0.5					
	Price negotiation	0.5					
	Purchase approval process	1.0					
Platform Installation		0.0					
Integration	Infrastructure modification	1.0					
	Appliance integration	1.0					
	MTA/MX configuration	1.0					
Configuration	Initial feature configuration	4.0					
Monitoring <sup>i</sup>	Monitoring of output/activities	35.0	35.0	35.0			
	Recurring configuration adjustments	35.0	35.0	35.0			
Upgrading <sup>ii</sup>	Upgrade planning, purchase, and procurement		2.0			£658	
	Upgrade integration		6.0				
Patching	Biannual patch integration	8.0	8.0	8.0			
End of Life	Infrastructure modification			1.0			
	Appliance de-integration			1.0			
	MTA/MX configuration			1.0			
	Total Hours	109	86	81			
	Total Cost of Hours	£4,340	£3,424	£3,225			
	Total Purchase Price				£5,289	£1,949	£1,291
	Three Year TCO						<b>£19,516</b>
	Annualised TCO						<b>£6,505</b>

## Postini - Total Cost of Ownership

Figure 2 below details the TCO of using the Postini service in a small network environment.

As Postini employs a service model, there are no costs associated with hardware, equipment replacement, signature/rule update services, or monitoring and management of a device. There is also no cost associated with platform installation, and fewer hours are associated with integration. The annual user-based license list cost and the activation fee are accounted for under the purchase variable.

Figure 2 : Postini Total Cost of Ownership for a Small Environment

TCO Factor	Activities/Details	Hours Year 1	Hours Year 2	Hours Year 3	Purchase Price Year 1	Purchase Price Year 2	Purchase Price Year 3
Planning	Review available options/features	16.0					
	Perform TCO analysis	3.0					
	Delegate responsibilities	1.0					
	Modify security policy	2.0					
Purchase	Annual per user licensing activation fee				£4,800 £599	£4,800	£4,800
Procurement	Distributor/vendor contact	0.5					
	Price negotiation	0.5					
	Purchase approval process	1.0					
Platform Installation		0.0					
Integration	Infrastructure modification	0.5					
	Appliance integration MTA/MX configuration	0.5					
Configuration	Initial feature configuration	1.0					
Monitoring <sup>1</sup>	Monitoring of output/activities	4.5	4.5	4.5			
	Recurring configuration adjustments	4.5	4.5	4.5			
Upgrading	Upgrade planning, purchase, and procurement						
Patching	Upgrade integration						
End of Life	Biannual patch integration						
	Infrastructure modification						
	Appliance de-integration MTA/MX configuration			0.5			
	<b>Total Hours</b>	<b>35</b>	<b>9</b>	<b>9.5</b>			
	<b>Total Cost of Hours</b>	<b>£1,393</b>	<b>£358</b>	<b>£378</b>			
	<b>Total Purchase Price</b>				<b>£5,399</b>	<b>£4,800</b>	<b>£4,800</b>
	<b>Three Year TCO</b>						<b>£17,129</b>
	<b>Annualised TCO</b>						<b>£5,710</b>

## Large Environment Cost

### TCO Variables and Considerations

For this large environment analysis, Frost & Sullivan has compared the integration of an e-mail security software solution with the cost of the Postini service.

An estimated number of hours is listed for each of the TCO variables discussed previously. The large environment analysis will assume a total of 10,000 mailboxes on a single site, with a fault-tolerant, high-availability e-mail security solution. Also included in the figures are the tangible list costs of hardware and the associated annual licensing fees for software that would be paid to an e-mail security software vendor, or the per user licensing and activation fees that would be paid to Postini. Because of the size and cost of the large environment solution, hours associated with planning, procurement, and configuration are increased.

*"Competitor B" - Total Cost of Ownership*

Figure 3 details the TCO of leveraging an e-mail security software solution in a large network environment.

Costs associated with software installation and server hardening are accounted for in the platform integration section.

Figure 3: "Competitor B" Total Cost of Ownership for a Large Environment

TCO Factor	Activities/Details	Hours Year 1	Hours Year 2	Hours Year 3	Purchase Price Year 1	Purchase Price Year 2	Purchase Price Year 3
Planning	Review available options/features	25.0					
	Perform TCO analysis	3.0					
	Delegate responsibilities	1.0					
	Modify security policy	2.0					
Purchase	Servers	1.0			£4,934		
	Licenses	1.0			£144,514	£144,514	£144,514
Procurement	Distributor/vendor contact	1.0					
	Price negotiation	3.0					
	Purchase approval process	4.0					
Platform Installation	Server hardening	12.0					
	Software installation	2.0					
Integration	Infrastructure modification	1.0					
	Server integration	1.0					
	MTA/MX configuration	1.0					
Configuration	Initial feature configuration	10.0					
Monitoring	Monitoring of output/activities	52.0	52.0	52.0			
	Recurring configuration adjustments	52.0	52.0	52.0			
Upgrading	Upgrade planning, purchase and procurement		2.0				
	Upgrade integration		6.0				
Patching	Biannual patch integration	8.0	8.0	8.0			
End of Life	Infrastructure modification			1.0			
	Server de-integration			1.0			
	MTA/MX configuration			1.0			
	<b>Total Hours</b>	<b>180</b>	<b>120</b>	<b>115</b>			
	<b>Total Cost of Hours</b>	<b>£7,166</b>	<b>£4,777</b>	<b>£4,578</b>			
	<b>Total Purchase Price</b>				<b>£149,447</b>	<b>£144,514</b>	<b>£144,514</b>
	<b>Three Year TCO</b>						<b>£454,997</b>
	<b>Annualised TCO</b>						<b>£151,666</b>

*Postini - Total Cost of Ownership*

Figure 4 below details the TCO of using the Postini service in a large network environment.

Since Postini employs a service model, there are no costs associated with hardware, equipment replacement, or the monitoring and management of a device. There is also no cost associated with platform installation, and fewer hours are associated with integration. The annual user-based license list cost and the activation fee are accounted for under the purchase variable.

Figure 4: Postini Total Cost of Ownership for a Large Environment

TCO Factor	Activities/Details	Hours Year 1	Hours Year 2	Hours Year 3	Purchase Price Year 1	Purchase Price Year 2	Purchase Price Year 3
Planning	Review available options/features	16.0					
	Perform TCO analysis	3.0					
	Delegate responsibilities	1.0					
	Modify security policy	2.0					
Purchase	Annual per user licensing activation fee				£100,000 £3,699	£100,000	£100,000
Procurement	Distributor/vendor contact	0.5					
	Price negotiation	1.5					
	Purchase approval process	4.0					
Platform Installation		0.0					
Integration	Infrastructure modification	1.0					
	Appliance integration MTA/MX configuration	1.0					
Configuration	Initial feature configuration	2.0					
Monitoring <sup>i</sup>	Monitoring of output/activities	17	17	17			
	Recurring configuration adjustments	17	17	17			
Upgrading	Upgrade planning, purchase, and procurement						
	Upgrade integration						
Patching	Biannual patch integration						
End of Life	Infrastructure modification						
	Appliance de-integration MTA/MX configuration			1.0			
	<b>Total Hours</b>	<b>66</b>	<b>34</b>	<b>35</b>			
	<b>Total Cost of Hours</b>	<b>£2,628</b>	<b>£1,354</b>	<b>£1,393</b>			
	<b>Total Purchase Price</b>				<b>£103,699</b>	<b>£100,000</b>	<b>£100,000</b>
	<b>Three Year TCO</b>						<b>£309,074</b>
	<b>Annualised TCO</b>						<b>£103,025</b>

## CONCLUSIONS

The statistics in the previous tables offer a comparison of the costs associated with using a product or service model. However, these models assume the use of a single site for an organisation. Even small- and medium-size organisations often install e-mail servers at multiple locations. In such a scenario, additional equipment must be purchased, configured, installed and monitored at these alternate sites. This is where the Postini service model shines brilliantly, because there is no hardware to install. Note in Figure 5 below, how shifting the cost analysis from one site to two not only increases the purchase price of equipment and related subscriptions, but doubles the integration, configuration, monitoring, upgrading, patching, and end of life TCO tasks.

An organisation with e-mail servers in three locations triples these costs, but the Postini costs merely increase by a few hours of integration and end of life tasks; preventing the costs of multiple locations from spiralling out of control.

Figure 5: Total Cost of Ownership for Single and Multiple Sites

Scenario	Single Site Fault Tolerant	Dual Sites Fault Tolerant	Three Sites Fault Tolerant
Competitor A 300 users	£19,516	£38,077	£56,637
Postini 300 users	£17,129	£18,303	£19,478
Competitor B 10,000 users	£454,997	£474,263	£493,529
Postini 10,000 users	£309,074	£313,334	£317,593

Although these cost comparisons generate some actionable statistics, they still fail to account for several other possible TCO factors. Additional value can be gained from Postini features such as e-mail spooling, which caches e-mail in the event that a client's mail server fails or is unreachable, and from Postini's user configuration capabilities, which preclude the need for administrators to bear the responsibility of such a dynamic policy. Many medium-size and even some small-size Postini clients have cited savings realised by foregoing further investments in e-mail servers and gateways, since the traffic is filtered and reduced before it reaches the client's perimeter. However, perhaps one of the most difficult duties is to estimate is the opportunity cost of the tasks that administrators could be working on instead of building and maintaining an e-mail security solution. With this factor, customers realise the full value of outsourcing, as it frees their internal resources to be spent working on their core competencies and other IT projects.

i Assumes 40 minutes per week of device monitoring activities to ensure the health of the device and 40 minutes per week of recurring configuration adjustment activities.

ii Assumes upgrades are available and are implemented once every two years.

iii Assumes five minutes per week of activity monitoring and five minutes per week of recurring configuration adjustment activities.

iv Assumes one hour per week of device monitoring activities to ensure the health of the device and one hour per week of recurring configuration adjustment activities.

v Assumes ten minutes per week of activity monitoring and ten minutes per week of recurring configuration adjustment activities.

vi [http://www.usatoday.com/tech/news/2004-01-26-managetech\\_x.htm](http://www.usatoday.com/tech/news/2004-01-26-managetech_x.htm)

## CONTACT US

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

**Silicon Valley**  
2400 Geng Road, Suite 201  
Palo Alto, CA 94303  
Tel 650.475.4500  
Fax 650.475.1570

**San Antonio**  
7550 West Interstate 10, Suite 400,  
San Antonio, Texas 78229-5616  
Tel 210.348.1000  
Fax 210.348.1003

**London**  
4, Grosvenor Gardens,  
London SW1W 0DH, UK  
Tel 44(0)20 7730 3438  
Fax 44(0)20 7730 3343

**877.GoFrost**  
[myfrost@frost.com](mailto:myfrost@frost.com)  
<http://www.frost.com>

### ABOUT FROST & SULLIVAN

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies, and the investment community, by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics, and demographics. For more information, visit <http://www.frost.com>.