

A Guide to Understanding Hosted and Managed Messaging

An Osterman Research White Paper

Published August 2007

SPONSORED BY



Contents

Why This Document Will be Worth Your Time	1
How Should Messaging be Managed?	1
Rising Costs	2
More Organizations are Considering Hosted and Managed Services	3
Market Overview	3
Proponents of Hosted and Managed Messaging	4
Detractors of Hosted and Managed Messaging	5
Who's Right?	5
Why Consider Hosted and Managed Services?	6
More Efficient Use of IT Resources	6
Potentially Lower and More Predictable Cost of Ownership	6
Flexibility of Deployment Options	8
Extending the Life of Existing Email Solutions	8
Disaster Recovery for Customer Systems	9
Business Continuity	9
Rapid Deployment of Services	9
Maintenance of the Most Current Capabilities	9
Many Providers Offer a Complete Range of Services	10
Very High Reliability and SLA Commitments	10
Excess Mail Capacity to Handle Unforeseen Problems	10
Minimizing the Impact on the Internal Network	10
Smooth Migration to New Messaging Platforms	11
Access to Expertise That Might Not Otherwise be Available	11
Good Physical Security	11
Privacy Guarantees	11
Vendor Independence	12
Questions to Ask of Your Internal Management and Hosted and Managed Service Providers	12
Questions to Ask Your Internal Management	12
Capabilities Offered	13
Architectural Considerations	13
Reliability	14
Security	14
Data Management	14
Services Offered	14
Vendor-Specific Questions	15
Migrating Away from the Vendor	16
Other Questions	16
Summary	16
Sponsor of this White Paper	17

Why This Document Will be Worth Your Time

Electronic messaging has become the de facto communications medium and file transport system used in the workplace today. Most information workers rely on email more than they do the telephone, fax or paper-based communication. The vast majority of organizations use email for sending, receiving and storing critical business records, including purchase orders, contracts, requests for proposal and other content. Instant messaging (IM) use is also on the increase, as are Web-based tools for communication and collaboration.

Consequently, messaging – particularly email – has become absolutely critical to the operation of most enterprises and has become something of a utility, much like electricity or water provision in certain key respects:

Messaging has become absolutely critical to the operation of most enterprises and has become something of a utility, much like electricity or water provision in certain key respects.

- It must be available at all times,
- It must meet anticipated and unanticipated spikes in demand, and
- Its cost should be driven as low as possible

How Should Messaging be Managed?

Organizations can manage their messaging functionality in one of three ways:

- Completely internally using in-house staff, hardware and software.
- Completely externally, using hosted or managed service providers for all messaging functions.
- Through the use of a hybrid approach in which some functions are managed internally and some are managed by a third party.

The purpose of this document is to offer an unbiased discussion and analysis of the key elements that must be considered by decision makers as they evaluate options for managing their messaging systems. Its goal is to inform decision makers about the benefits of using a hosted or managed messaging service and the key questions to ask of any provider of a single messaging service or a complete suite of services.

Rising Costs

Maintaining messaging functionality is not a trivial expense. Depending on an organization's specific requirements, the number of email users it supports, the geographic distribution of its employees and other factors, the total cost of ownership for a messaging system is anywhere from \$15 to \$50 per seat per month and can be much more in some cases. Further complicating the problem is that messaging costs are not as predictable as many decision makers would like them to be – a power outage, the outbreak of a new worm or the loss of key personnel can all drive up the cost of messaging unexpectedly.

Among the factors that are serving to drive up the costs of messaging are:

- The need to overspecify email systems to handle mail volume spikes from denial-of-service attacks, dictionary harvest attacks and other threats.
- Deploying more servers, appliances, storage systems, bandwidth and other hardware and software to deal with growing volumes of spam, viruses, spyware and other problems.
- Deploying content-scanning systems that can monitor outbound email, instant messages, blog posts and other content for potential policy violations, data breaches and other risks that could pose a threat to an organization.
- Deploying technology to improve the reliability and resiliency of messaging systems in order to provide as much uptime as possible.
- Hiring IT personnel knowledgeable enough to maintain the systems in-house and training them on future hardware and software releases.
- Patching various servers, appliances and other on-premise systems and managing the unexpected problems that may arise from a patch's impact on another system. This becomes more difficult in larger companies, particularly those that have a geographically distributed infrastructure.
- Implementing business continuity and disaster recovery capabilities to ensure that an organization can recover

The total cost of ownership for a messaging system is anywhere from \$15 to \$50 per seat per month and can be much more in some cases. Further complicating the problem is that messaging costs are not as predictable as many decision makers would like them to be.

as quickly as possible from any of the variety of problems that can bring down its messaging capability.

- Adding more storage and storage-related systems in order to accommodate the rapidly growing quantity of messaging system content.
- Deploying e-discovery and regulatory compliance capabilities that are designed to mitigate an organization's risk from non-compliance with the growing array of legal and regulatory requirements focused on messaging and other electronic content.
- The need to deploy encrypted messaging capabilities.
- Deploying and managing mobile messaging platforms and supporting users of these devices.

In short, providing messaging services is expensive, somewhat unpredictable and it will be more expensive in the future.

More Organizations are Considering Hosted and Managed Services

During the past several years, the market for hosted and managed messaging services has increased substantially. Osterman Research anticipates that the market will continue to grow at a healthy pace as an increasing proportion of organizations realize the benefits of allowing specialist providers to manage some or all of the corporate messaging infrastructure.

It is important to note that many organizations are finding benefit in using a hybrid approach, in which some functions are managed using on-premise capabilities, while some functions are provided by a hosted or managed solution. Using a hosted perimeter email protection service, for example, can eliminate most spam before it ever hits the corporate network, eliminating much of the storage and bandwidth requirement for on-premise systems.

Market Overview

Based on a major study of mid-sized and large organizations that Osterman Research conducted during June 2007, we forecast increasing penetration of hosted and managed services in the North American market through 2009 as

Based on a major study of mid-sized and large organizations that Osterman Research conducted during June 2007, we forecast increasing penetration of hosted and managed services in the North American market through 2009.

shown in the following table. It is important to note that the last three offerings in the table may be included as part of a hosted or managed email service, or they may be used to supplement on-premise messaging capabilities.

**Percentage of North American Organizations
That Will be Using a Hosted or Managed Solution**

Messaging Function	2007	2008	2009
Hosted email services (e.g., hosted Exchange)	13%	14%	19%
Anti-virus and anti-spam	22%	29%	32%
Email retention and archiving	14%	24%	31%
Wireless/mobility services	21%	21%	27%

Hosted and managed messaging services are clearly a growing market, but one that is characterized by very strong opinions from both proponents and detractors of the hosted/managed paradigm.

Hosted and managed messaging services are clearly a growing market, but one that is characterized by very strong opinions from both proponents and detractors of the hosted/managed paradigm.

Proponents of Hosted and Managed Messaging

Proponents of hosted and managed messaging services argue that it makes sense to let a specialist organization manage these services, since these vendors can achieve economies of scale that many firms, particularly smaller ones, could never hope to achieve. To help ensure messaging continuity, these providers operate multiple data centers that are physically secure, have diesel backup generators, use redundant communications links, provide a full complement of staff on a 24x7 basis, create redundant copies of data for storage at geographically separated sites, and offer other capabilities that are fully managed.

For messaging security services, anti-virus signatures are updated continually, multiple anti-virus and anti-spam capabilities are typically employed, and these scanning engines are tuned and updated by the security vendor, allowing customers to leverage the security vendor's expertise. Further, managed security providers can spool email in case their customers' primary email servers go down, or they can provide more robust disaster recovery services, enabling business continuity and disaster recovery for their customers.

For messaging archiving and data management services, service providers offer extremely high levels of reliability and so capture all messaging content, even when on-premise

systems are down, allowing total compliance with corporate retention policies.

For other types of services, such as wireless/mobility services, hosted and managed services provide very high reliability even when the primary corporate system is down. This allows mobile employees to communicate even when the primary in-house messaging system is unavailable.

In a hosted environment small and mid-sized businesses (SMBs) now have the opportunity to utilize the features and functionality of best-of-breed messaging services at a low per-user price. Previously, these applications have been accessible only to Fortune 500 companies because the latter have the economies of scale to implement these capabilities.

Detractors of Hosted and Managed Messaging

Those who oppose the use of hosted and managed services argue that messaging is a core and fundamental skill set that must be maintained in-house for a variety of reasons. They argue that internal management of the messaging infrastructure, including messaging security, is less expensive than if a managed service provider is employed for this purpose. The corporate message store, which represents the primary content store for most organizations and its most important data asset, is simply too valuable to be managed by a third party at a remote data center. They further argue that security of the messaging repository requires that it be managed behind the corporate firewall. Further, newer software-based and appliance offerings from a variety of leading and other vendors require little investment by IT staff for activities like deployment, upgrades, patch management and the like, and so the cost of managing a messaging system internally is being driven lower over time.

Who's Right?

Given the importance of messaging functionality to virtually all organizations, deciding on the best way to manage this critical corporate asset is not a trivial decision. Because email is the primary communications and file transport mechanism for virtually all organizations, managing this capability efficiently and properly is becoming increasingly critical. Also, as instant messaging, Web collaboration, VoIP and other capabilities become more widely used in the workplace, the decision about how best to manage a messaging infrastructure will become ever more important.

Given the importance of messaging functionality to virtually all organizations, deciding on the best way to manage this critical corporate asset is not a trivial decision.

Why Consider Hosted and Managed Services?

Why should your organization consider the use of a hosted or managed messaging service? There are a variety of reasons to at least consider using such services, some of which, as discussed below, may provide important benefits compared to current, internal methods of managing these capabilities.

More Efficient Use of IT Resources

One of the fundamental issues that should be considered by any organization – but one that often is not – is that of the opportunity cost of IT staff members. Most CIOs and IT managers would agree that finding and retaining highly qualified IT staff is not an easy task, particularly in a good economy when competition for good IT talent is robust. Consequently, in-house IT staff should be used in a way that allows them to provide maximum benefit to their employer, while at the same time affording them a satisfying work experience that will motivate them not to move elsewhere.

A hosted or managed messaging service – whether used for messaging security, archiving, encryption or other tasks – can free IT staff members from the relatively mundane tasks associated with managing internal systems. This allows them to be deployed on initiatives that provide more differential value to the organization and that can result in greater job satisfaction. For example, if an IT staff member can manage a messaging capability extraordinarily well, he or she provides some level of value to the enterprise. However, if that staff member spent the same amount of time integrating customer-facing IM capabilities into the company's technical support system, it is very likely that much greater value could be realized from the same level of effort, not to mention that the latter project would likely provide greater job satisfaction.

In a broader context, the use of hosted or managed services allows an organization to focus more on its core business rather than devote resources to managing its messaging infrastructure. Just like the vast majority of organizations do not generate their own electricity or drill their own wells, organizations should consider messaging to be a utility service that a specialist provider may be better equipped to manage.

Potentially Lower and More Predictable Cost of Ownership

There is a widely held perception that internally managed messaging systems are less expensive to deploy and

A hosted or managed messaging service – whether used for messaging security, archiving, encryption or other tasks – can free IT staff members from the relatively mundane tasks associated with managing internal systems.

operate than hosted or managed services. While in some cases that perception is accurate, very often it is not for two reasons:

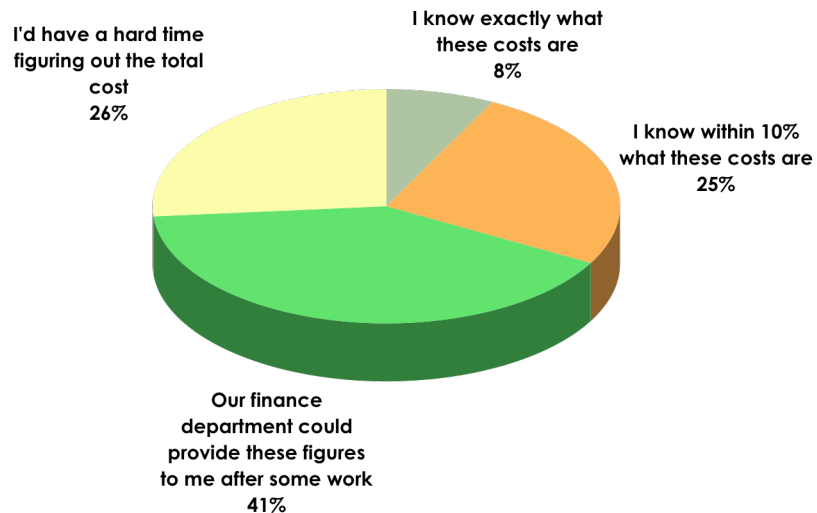
- First, many decision makers do not consider the *complete* cost of providing messaging functionality within their organization. They often underestimate the total amount of labor required to manage the system, the disruptive impact of outages and other unforeseen events on other activities, the true costs of capital expenditures, the unexpected costs of managing a system, and so forth.
- Second, most decision makers simply do not know what it costs their organization to provide messaging services. In a June 2007 Osterman Research survey, for example, we asked messaging decision makers the following question:

'How closely do you track the total cost of your messaging system, including licenses, hardware depreciation, maintenance/support contracts, personnel, backups, etc?'

Their responses are shown in the following figure.

Many decision makers do not consider the complete cost of providing messaging functionality within their organization. They often underestimate the total amount of labor required to manage the system, the disruptive impact of outages and other unforeseen events on other activities, the true costs of capital expenditures, the unexpected costs of managing a system, and so forth.

"How closely do you track the total cost of your messaging system?"



Flexibility of Deployment Options

One of the benefits of using a hosted or managed messaging service is that it allows an organization to adopt a granular approach in how it manages its messaging capabilities. For example, an organization that uses appliances to protect its infrastructure from spam and viruses can adopt a hybrid approach in which it uses a hosted reputation service to block the bulk of spam and viruses entering the network, thereby dramatically reducing the impact on internal storage and bandwidth, but continue to use its internal appliances for spam and virus filtering. An organization may decide to manage its own email servers for employees at a corporate headquarters, but use a hosted messaging service for employees in field offices. An organization may want to supplement its primary internal archiving system with a hosted solution for remote employees.

One of the benefits of using a hosted or managed messaging service is that it allows an organization to adopt a granular approach in how it manages its messaging capabilities.

In short, hosted and managed solutions allow organizations to exercise a great deal of flexibility in how they manage their messaging infrastructure, supplementing or replacing internal capabilities quickly and painlessly.

Extending the Life of Existing Email Solutions

Related to the point above is that hosted and managed services allow an organization to extend the useful life of an in-house messaging solution. For example, if a company has reached the maximum capacity of its email filtering appliances because of rapidly growing spam volumes, it could implement a hosted email security service that would dramatically reduce the amount of incoming traffic and thereby allow new investments in internal hardware to be delayed or, possibly, avoided.

For example, the enormous increase in the volume of spam during 2006 driven by botnets and the use of image spam resulted in many on-premise solutions reaching their maximum capacity. Faced with such a predicament, an organization could use a hosted service to supplement its internal capabilities and thereby preserve its investment in the on-premise solutions it has deployed, thereby extending the useful life of these systems. This would allow an organization to start using hosted services in a supplementary role, allowing the organization to determine whether or not hosted or managed services would fit into their future plans.

Disaster Recovery for Customer Systems

Most hosted and managed service providers offer some level of disaster recovery. For example, most hosted security providers will spool email for at least several days in the event that a customer's email servers go down. This ensures that email sent to the customer will not be bounced back to the sender and that email will continue to be received until the customer's email servers are restored.

Business Continuity

Even more important, however, is some providers' provision of business continuity capabilities on a number of levels, including backup email systems, continued archiving of messaging system content during outages and other services. This allows messaging capabilities to remain active regardless of problems that may occur at their customers' sites. Using such a business continuity service will allow a business to recover much more quickly from a power outage, a natural disaster or some other disruptive event.

Rapid Deployment of Services

One of the fundamental benefits of a hosted or managed service is the speed with which services can be deployed. For example, deploying new hosted or managed services typically requires no more than the change of an MX record or a change in the configuration of messaging clients. Adding new users to an existing service typically requires just a phone call, completion of an online form or it can be accomplished through a Web-based administration tool. Hosted and managed services make it easy to add or subtract small numbers of users, or even entire business units, from a particular service, which is particularly advantageous when integrating merged or acquired companies into a messaging infrastructure.

Maintenance of the Most Current Capabilities

Hosted and managed service providers typically update their capabilities on a near real-time basis. For example, a hosted or managed archiving services provider can implement a new retention policy immediately for all of its customers. A provider of anti-virus and anti-spam filtering services will typically update its signatures on a continual basis. Further, service providers typically deploy a broader range of leading technologies and offer expertise that might not otherwise be available or affordable to their customers, particularly their smaller customers.

One of the fundamental benefits of a hosted or managed service is the speed with which services can be deployed. For example, deploying new hosted or managed services typically requires no more than the change of an MX record or a change in the configuration of messaging clients.

Many Providers Offer a Complete Range of Services

One of the more important advantages of a hosted or managed service is that many can offer a complete range of services, including Exchange, Notes, GroupWise, POP, IMAP, Webmail or other messaging services; message filtering for spam, viruses and malware; archiving of inbound and outbound content; encryption; email continuity services in the event of a failure in the primary email system; compliance with regulatory and e-discovery requirements; IM filtering; and data migration services. Alternatively, a single service can be employed initially and other services added as corporate requirements change.

Very High Reliability and SLA Commitments

Hosted and managed services vendors can typically invest more resources into their infrastructure than individual organizations can afford and so provide extremely high levels of reliability. Because most hosted and managed service providers maintain very robust data centers, they can typically offer very high levels of reliability and Service Level Agreements (SLAs) that would be difficult for internally managed systems to match. This allows customers to focus on providing services that offer greater value to their enterprise with the assurance that messaging functionality will be available virtually 100% of the time.

It is also important to consider that hosted and managed providers' data centers are staffed on a 24x7 basis and that capabilities are monitored around the clock. This means that problems can be dealt with more rapidly than is feasible in many on-premise deployments.

Excess Mail Capacity to Handle Unforeseen Problems

Hosted and managed messaging providers typically have much more excess mail capacity than an organization that manages its own on-premise email infrastructure. This is simply because it is not economically feasible for the latter to deploy enough excess capacity to maintain in the event of a crippling, large-scale spam attack, for example. Excess capacity deployed for a large number of customers is simply more economically feasible for a service provider.

Minimizing the Impact on the Internal Network

Because such a high percentage of malicious spam is not directed to valid email addresses, using a perimeter-based service offloads the majority of email processing (and associated email network traffic) before it ever reaches the customer's network. On-premise solutions, regardless of how

Hosted and managed providers' data centers are staffed on a 24x7 basis and that capabilities are monitored around the clock. This means that problems can be dealt with more rapidly than is feasible in many on-premise deployments.

robust, still must react to spam after it has entered the network, placing additional demands on storage and bandwidth.

Smooth Migration to New Messaging Platforms

Among the chief benefits offered by a hosted or managed service is that migration to new messaging systems is made much easier. For example, while migrating from Microsoft Exchange 2003 to Exchange 2007 will offer a number of benefits because of the improvements designed into the latter, migrating to the system using internal resources is a significant undertaking because of the need to implement 64-bit hardware, the deployment of new server software, the time required to learn the new server roles in Exchange 2007, etc. Using a hosted or managed service provider that will migrate to the next-generation messaging capability for its customers is substantially easier and less painful than an internal migration.

Access to Expertise That Might Not Otherwise be Available

Specialist providers of hosted and managed services can often provide expertise, such as professional services for migration, that might not otherwise be available. This is particularly advantageous for smaller companies.

Good Physical Security

One of the concerns that many prospective customers of hosted and managed services express is focused on the physical security of their data when managed by a third party. Most of the leading providers of hosted and managed services maintain very secure physical facilities, including video surveillance, multiple access points using two-factor authentication, tracking and monitoring tools and other systems that protect their customers' data from being compromised. Measures, such as SAS 70 audits or WebTrust certification, can provide an extra level of assurance for customers.

Privacy Guarantees

Some organizations are concerned with the privacy of their messages when routing them through a hosted or managed service. However, messages are generally automatically processed by the system without any human intervention. Messages are normally stored only to benefit the customer, such as through quarantines or for disaster recovery measures.

Most of the leading providers of hosted and managed services maintain very secure physical facilities, including video surveillance, multiple access points using two-factor authentication, tracking and monitoring tools and other systems that protect their customers' data from being

Vendor Independence

Using a hosted or managed service provider can make a customer of the service less dependent on a particular vendor's technology, and so will minimize the impact of legacy systems on future technology or vendor choices.

Questions to Ask of Your Internal Management and Hosted and Managed Service Vendors

There are a number of questions that any prospective customer of hosted or managed messaging services should ask of a vendor they are considering to provide these services. There are also several questions that organizations should ask themselves before they use a third party to provide messaging services.

The following offers a good starting point for questions that should be asked, although it is important to note that not all of the questions will apply to all types of hosted and managed services or to all vendors.

Questions to Ask Your Internal Management

- **Is messaging a core competency that we want to retain in-house?**
- **Do we have enough IT staff members, or will we be able to recruit enough IT staff, to manage our current and planned messaging capabilities, as well as other IT initiatives from which we could derive competitive advantage?**
- **How much will it cost us to deploy all of the new capabilities that we will need for archiving, encryption, security and other capabilities over the next few years?**
- **What is the total cost of managing our messaging infrastructure, including whatever opportunity costs may be associated with managing our systems internally?**
- **How much will it cost us to migrate to a new messaging system when such a migration is required?**

There are a number of questions that any prospective customer of hosted or managed messaging services should ask of a vendor they are considering to provide these services. There are also several questions that organizations should ask themselves before they use a third party to provide messaging services.

Capabilities Offered

- **What capabilities does the vendor offer today and what capabilities are on the vendor's roadmap? These services might include:**
 - Hosted messaging services
 - Archiving
 - Online backup
 - Encryption
 - Unified messaging
 - Mobility
 - Web conferencing and other collaboration capabilities
 - Instant messaging services
 - Active Directory integration
 - Other capabilities
- **Which email servers / platforms are supported?**
- **Which versions of email servers and platforms are supported?**
- **Which email clients are supported?**
- **Does the vendor provide real-time scanning of Web traffic for viruses and malware?**
- **Does the vendor support or require any on-premise hardware or software?**
- **How many data centers does the vendor operate?**
- **What type of data center is provided?**
- **What migration tools and services are offered?**
- **How often are upgrades provided?**
- **What reporting capabilities are provided?**
- **Does the vendor have premier support agreements with their technology partners?**
- **Are disaster recovery services offered if the customer system is unavailable?**

What architectural capabilities ensure that there is neither delay in message delivery nor any additional, unnecessary risk incurred by storing a copy of the message?

Architectural Considerations

- **What architectural capabilities ensure that there is neither delay in message delivery nor any additional, unnecessary risk incurred by storing a copy of the message?**
- **Does the vendor perform full, nightly backups of customer data?**

- **Is the vendor using their own technology or another vendor's?**
- **Does the vendor use the application developer's platform or one developed by another vendor?**
- **Will the vendor's infrastructure scale to meet future requirements?**

Reliability

- **What Service Level Agreements does the vendor offer?**
- **How much system downtime has the vendor experienced during the past month? Six months? Year?**

Security

- **How secure is the infrastructure?**
 - What controls are in place to control access to customer data?
 - What intrusion detection systems are in place to protect the vendor's data center?
 - What redundant capabilities are in place, including backup generators, redundant telecommunication links, etc.?

What Service Level Agreements does the vendor offer?

How much system downtime has the vendor experienced during the past month? Six months? Year?

Data Management

- **Does the vendor host customers on shared and/or dedicated servers?**
- **In what countries will the data be stored?**

Services Offered

- **How integrated are the services? For example, if the vendor offers IM and archiving services, are instant messages archived?**
- **Does the vendor provide other complementary products and services?**
- **Does the vendor provide both shared and dedicated servers?**
- **What customer support services are offered?**
 - What are the technical support hours?
 - Does the vendor offer live 24x7 support?
 - Where are the technical support staff based?

- **Does the vendor provide a dedicated Technical Account Manager after the sale?**
- **Can customers outsource DNS, Web sites and applications, and email to the vendor?**
- **Can customers resell the service? If so, what features are offered to support reselling the service (white labeling, reseller's console, etc.)?**
- **What provisioning tools are provided?**
- **Does the vendor provide automated Web services?**
- **How flexible is the provider in offering various services?**
- **Are policies across all communications channels unified and managed in a single, integrated Web console?**
- **Is distributed administration of the service supported (e.g. regional administrators with control over only a subset of the users)?**
- **Are end-users able to manage their own configurations and settings?**
- **Are messages stored on disk and then forwarded to the end customers?**

How long has the vendor been in the specific business for which they are being considered (security, archiving, complete messaging services, encryption, etc.)?

Vendor-Specific Questions

- **Is the vendor financially viable?**
- **How long has the vendor been in the hosting or managed services business?**
- **How long has the vendor been in the specific business for which they are being considered (security, archiving, complete messaging services, encryption, etc.)?**
- **How many customers does the vendor support and how has this changed?**
- **What size and type of customers does the vendor support?**
- **Can the vendor provide referenceable customers that are similar to our organization?**
- **What email volume does the vendor support and how has this changed?**

- **What certifications have the vendor's employees earned? How many?**
- **What corporate certifications or audits are offered?**

Migrating Away from the Vendor

- **What are the termination conditions?**
- **How can data be exported / migrated to an on-premise solution or to another hosted provider?**

Other Questions

- **Does the vendor offer professional services?**
- **What is the experience level of the vendor's professional services team?**
- **Who will own our data?**

Summary

Messaging is a mission-critical function for virtually all organizations and it is becoming more so. However, managing messaging systems is becoming more difficult and more demands are being placed on organizations to manage these systems effectively.

One option that can help organizations to manage their messaging systems more effectively is the use of hosted or managed services to provide some or all of the services they require. Although many corporate decision-makers balk at the prospect of using a hosted or managed service because they perceive these services to be more expensive, less secure or offer less control compared to on-premise systems, Osterman Research has found that these fears are, in almost every case, unfounded. On the contrary, hosted and managed services often are less expensive than on-premise systems, provide better security than has been deployed in most companies, and offer at least as much control over the data.

There are a number of issues to consider for organizations that are evaluating hosted or managed service providers. Due diligence in evaluating the hosted/managed option can yield significant benefits and will be worth the effort.

There are a number of issues to consider for organizations that are evaluating hosted or managed service providers. Due diligence in evaluating the hosted/managed option can yield significant benefits and will be worth the effort.



1600 Amphitheatre Pkwy.
Mountain View, CA 94043

Toll Free (US/Canada)
+1 866 767 8461

Toll Free (Germany)
0800 67 37 97 6

Europe
+44 20 7082 2000

Other
+1 650 486 8100

www.google.com/a/security

Sponsor of this White Paper

Postini is a wholly owned subsidiary of Google, Inc. Google Apps is a suite of applications that includes Gmail, Google Calendar (shared calendaring), Google Talk (instant messaging and voice over IP), Google Docs & Spreadsheets (online document hosting and collaboration), Google Sites (team site creation and publishing), Start Page (a single, customizable access point for all applications) and Google Apps Security & Compliance. The security and compliance products, powered by Postini, are available to businesses and organizations who want to make their existing email infrastructures more secure, compliant and productive. Businesses of all sizes can now get best in class email security, archiving and e-discovery and Google Apps innovation is making it easier and more affordable than ever before. These products work with virtually any email server that supports SMTP such as Lotus Notes/Domino, Microsoft Exchange, Novell Groupwise and others.

© 2007 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.