

Moving to the Cloud

Important Things to Consider Before Migrating Your Messaging Infrastructure to the Cloud

Overview

Over the past several years “cloud computing” has been a hot topic on the minds of most IT executives because of the potential benefits cloud computing promises to deliver to enterprise organizations. The promises of:

- Lower costs
- Increased storage
- Higher automation (fewer IT personnel)
- Increased flexibility, and
- Allowing IT organizations to shift focus to strategic revenue-generating projects,

are some of the key drivers behind mandates from executives to move IT infrastructure from on-premises to the cloud.

But even though the many benefits of cloud computing are better understood by IT executives today, it's becoming painfully obvious that there are many more problems and compromises that need to be taken into consideration before outsourcing enterprise infrastructure to the cloud.

One area of IT infrastructure that has proven difficult to migrate to the cloud is the messaging infrastructure. The promises of cloud computing can potentially be realized by migrating certain components of the messaging infrastructure to the cloud; however, there are compromises and security issues that must be thoroughly considered before attempting to move email infrastructure to the cloud.

For example, the typical enterprise messaging infrastructure has some combination of the following three layers:

1. **Gateway: External Layer** — inbound malware filtering, simple routing and security
2. **Mail Store: Groupware Layer** — mail stores with simple policy and user-user message delivery
3. **Email Backbone: Internal Layer** — bi-directional policy and directory-driven security, enforcement and intelligent routing

Messaging cloud providers, including Microsoft® and Google™, advertise that all three layers can effectively be moved to the cloud.

Specifically, Microsoft Exchange 2010 is available as a cloud/SaaS offering called the “Business Productivity Online Suite,” or BPOS. BPOS includes Exchange Hosted Services and Collaboration Services. Together with Forefront®, Microsoft’s messaging security SaaS offering (message filtering, identity management), businesses can potentially move their entire email infrastructure (all three layers) to a Microsoft-controlled cloud.

Google also offers a cloud-based messaging “App” that includes Gmail™, Google Calendar™, messaging services (mail stores), and security and filtering using its Postini email solutions™ messaging product. Google advertises that it, too, can offer businesses a complete email solution in the cloud.

Both Microsoft and Google have been somewhat successful penetrating the enterprise with their cloud offerings, however, most of their successful customers are small-to-medium-sized businesses, and according to a recent Gartner report,¹ “the uptake in cloud e-mail services has been happening at a slower pace than previously expected.” There are many reasons for this including:

- Vendor dynamics (product delays, lack of migration tools, etc.)
- Economics (pricing and TCO)
- Service maturity (lack of hybrid options, functionality and security)

In addition, moving any layer of the messaging infrastructure to the cloud has proven to be much more complex than originally thought. In fact, nearly all of Sendmail's Fortune 1000 customers have discovered this to be true. Most of these customers have conducted a Messaging Architecture Review with Sendmail's

team of Messaging Architects. The reviews helped uncover a number of potential issues, and in some cases, discovered that the customer's email infrastructure could not be moved to the cloud without compromising functionality, compliance laws, security and more.

The following three sections outline key questions and findings that these Fortune 1000 businesses discovered during their Messaging Architecture Reviews. The findings are by no means a comprehensive list of all questions and issues that should be addressed, but instead they're focused on some of the more critical issues that have been discovered.

1. Outsourcing the External Gateway Filtering Layer

Overview

- Off-site hosting of anti-spam, anti-virus, IP reputation and basic policy enforcement to the cloud
- Replaces anti-spam/virus filtering appliances/servers in the on-premises DMZ gateway layer
- The Groupware layer is on-premises (Exchange, etc.)

Critical Things to Consider

The external gateway systems (typically in the DMZ) are still required for accepting inbound mail from the Internet SaaS provider, although for a large enterprise the number of gateway systems may be substantially reduced. The actual cost of outsourcing the filtering layer needs to be carefully calculated in addition to answering the following critical questions:

- Is TLS encryption important to your organization? It is likely that you will lose control over TLS encrypted sessions when filtering is done in the cloud. A few providers offer some level of "opportunistic" TLS encryption; however support for TLS authentication, which most enterprises require, is not managed by the cloud provider.
- Is S/MIME encryption important to your organization? As is the case with TLS encryption, you will also lose control over S/MIME gateway encryption. To date, no cloud messaging provider supports S/MIME gateway encryption, a de facto standard for implementing secure tunnels for email. End-users would be required to implement S/MIME at the desktop and there would be no way to implement server-side encryption policy for S/MIME. Among potential problems, you could lose the capability to virus scan S/MIME encrypted messages entering your organization before those messages reach the desktop.
- Are other methods of message encryption, such as Voltage IBE, important to your business? Some cloud providers support certain types of message encryption; however the ability to intelligently encrypt/decrypt messages needs to be driven by corporate policies. As some of Sendmail customers' have discovered, cloud filtering solutions, including those offered by Google and Microsoft, provide only simple email policy capabilities. In order to accomplish even basic policy enforcement, the cloud provider requires your Active Directory, and other LDAP sources, to be synchronized with their service — this alone raises serious security and privacy concerns for many companies.
- Is your company willing to compromise security for improved spam filtering? In order to provide optimum spam filtering, the cloud provider needs access to your corporate directories. For example, to perform recipient validation on inbound messages, the cloud provider requires an up-to-date list of all your valid email users, which raises serious security and privacy issues that must be well thought through before releasing this sensitive data to the cloud provider.
- Is it important for your IT/Help Desk to have access to email logs? You may lose the ability to access your email logs when using a cloud provider for message filtering. For example, tracking "lost" messages for end users may become very problematic if you don't have access to all of your email logs.
- Does your organization have special spam handling requirements? When outsourcing the spam filtering function, you may lose control of the ability to create special use-cases for spam handling.

Conclusion and Recommendations

- Depending on the specific requirements of your organization, outsourcing the filtering function can be problematic.
- If encryption is important to your organization, cloud offerings will prove to be difficult.
- If the cloud provider requires Directory data for improved spam handling and policy enforcement, you must consider the potential security risks of letting that data leave your organization.
- To avoid any of these potential problems, Sendmail always recommends that you conduct a thorough Messaging Architecture Review before outsourcing your external gateway filtering layer to the cloud.

2. Outsourcing the Groupware Layer

Overview

- Off-site hosting of groupware systems and mail stores (Exchange, POP/IMAP, etc.)
- The filtering layer is almost always outsourced before the groupware layer. This can be done with the same or different cloud provider.

Critical Things to Consider

In addition to the key considerations outlined in table 1, other important questions to consider before outsourcing this layer to the cloud include:

- Does your business have enterprise message routing requirements? Most large organizations have fairly complex routing requirements that are difficult to implement and manage if your groupware system is hosted. For example, many enterprises, especially those with multiple domains, often have complex 'message manipulation' requirements. These include things such as address header rewriting before delivering messages. They have enterprise routing requirements that must rely on sensitive Directory attributes to enforce. This level of message header manipulation and intelligent routing is difficult to implement in the cloud. In these cases an external gateway and/or an on-premises email backbone policy layer is always required; however, even then, message traffic between your organization and the cloud provider will increase substantially.
- Does your organization require sending of large messages and attachments that you know of? Even the large cloud providers such as Google have restrictions on the size of messages that it will handle. For example, pharmaceutical companies require the sending of very large messages.
- Does your company have strict archiving policies? Most enterprises, especially those that are highly regulated, have strict email archiving policies that are difficult to implement in the cloud. For example, financial services firms require that all email destined "outside the company" must be retained and messages between certain internal departments be archived. To accomplish this, LDAP attributes must be used to determine the correct policy on any given message. Is your company willing to give sensitive LDAP information to an external public cloud provider?
- Do you want potentially legal or damaging email to be archived, or even sitting in your end-users inbox, outside the control of your organization?
- Does your company have strict data retention policies? In the cloud, organizations lose control of data retention. While there may be options to make the data inaccessible to the customer after the retention policy, there is no control as to when the data is actually removed from all potential locations (databases, backups, logs, etc.). This can apply to messaging data as well as metadata such as logs.
- What level of trust will you have with your cloud provider? While an organization may trust their cloud provider, they may not know about other third-party partners of that provider. For example, cloud providers may use external storage or back-up providers. You should be aware of any partnerships at the time you establish a contract with the cloud provider, and you should be notified of any new partnerships during the duration of your contract.

- What about confidentiality? With the potential loss of encryption capabilities with cloud services, all data flowing through the provider can be reviewed by the provider or possibly their business partners.

Conclusion and Recommendations

- Enterprises have complex policy and email handling requirements that have proven to be problematic to implement and enforce in the cloud.
- To effectively enforce email policies, enterprises will need to give up certain aspects of the messaging security and policy handling that they currently have with their on-premises solutions. More often than not, this is an unacceptable proposition.
- In order to satisfy enterprise-level message policy and handling requirements, an on-premises external gateway and/or an on-premises email backbone policy layer is almost always required. If this is the case for your organization, and you outsource the groupware layer, this effectively means that the cloud provider is only hosting your message store - which by itself is often an issue—(see previous bullet).
- To avoid any of these potential problems, Sendmail always recommends that you conduct a thorough Messaging Architecture Review before outsourcing your groupware layer to the cloud.

3. Outsourcing the Email Backbone Internal Layer

Overview

- External gateway filtering and groupware layers typically will have been outsourced if the email backbone layer is even considered
- Inbound and outbound messages may still need to be managed internally
- This is the most difficult, if not impossible, layer to outsource for large enterprises

Critical Things to Consider

Virtually all of the issues outlined in tables 1 and 2 are also problematic when trying to outsource the email backbone layer to the cloud. For most enterprises it may be impossible to outsource this layer. Additional questions to consider include:

- Are there “email-generating” applications that IT does not centrally manage or control? Virtually all enterprises have applications that generate email. Examples include CRM systems, billing and invoice systems, trade confirmations, marketing systems, and many homegrown systems that the IT department may not even be completely aware of. These email-generating applications are often found on UNIX systems, Mainframes, Windows, etc. Most companies also have devices that use the internal messaging backbone to operate (copiers, scanners, printers, etc). These systems and devices rely on internal mail systems to operate and it may be difficult or even impossible to configure all of these applications and devices to use with the off-site, cloud-provided messaging systems.
- Does your company have complex message policy requirements? Businesses that are highly regulated by default have very complex message policy and routing requirements. Encryption, archiving, “Chinese Walls,” and disclaimers are just a few critical requirements that are very difficult to implement outside of the corporate walls. Again, LDAP directories are critical to help make sophisticated policy decisions, and large businesses with complex infrastructures and dozens of directory sources make it virtually impossible to outsource this function.
- What are your encryption requirements? As described in tables 1 and 2, message encryption decisions are almost always made based on LDAP attributes and the level of encryption support offered by cloud providers may not be sufficient.
- Do you have a need to “manipulate” message headers for outbound messages? Many large organizations, especially those that have multiple domains, have a requirement to rewrite message headers for outbound messages. For example, a bank that has multiple brands due to acquisitions and consolidation may require that all outbound email messages be “from” the parent bank (primary brand). This level of message

manipulation would be difficult to do in the cloud since policy decisions to determine which message headers should be re-written would be LDAP-driven. Again, releasing LDAP data to a cloud provider raises serious security and privacy issues and must be well thought through before agreeing to release it.

- Does your business require you to log and archive certain email communications? If you need complete control over logs and log management for reporting and compliance, you may not be able to outsource this layer. Access to off-site logs can be problematic, however even more importantly the immature policy capabilities of the cloud providers make it difficult to acquire the required logs for detailed and custom reporting for critical things such as compliance regulations.
- Can existing point product filtering appliances be used for this layer if the filtering layer has been moved to the cloud? Some businesses that have successfully moved their filtering and/or groupware layer to the cloud have tried to use point products that were designed for message filtering to handle the critical email backbone function. Most have discovered that products designed for filtering (Cisco Ironport, Proofpoint, Axway, etc.) are not capable of handling the complex message policy and routing functions of the internal email backbone.

Conclusion and Recommendations

- The internal email backbone has proven to be the most difficult layer of a messaging infrastructure to outsource.
- Most enterprises have a large number of email-generating applications that are difficult, if not impossible, to integrate with a cloud service provider.
- Businesses may need to give up certain aspects of the messaging security and policy enforcement capabilities they currently have with their on-premises solutions. More often than not, this is an unacceptable proposition.
- Sendmail recommends that all organizations conduct a thorough Messaging Architecture Review before moving any layer of their messaging infrastructure to the cloud. To date Sendmail has not seen a single enterprise messaging infrastructure that did not require an on-premises email backbone.

Conclusion

"At the time of the prediction, the "halo effect" of the cloud was undiminished and top management — both IT and top business management — assumed that e-mail was a commodity, and that the cloud was ready for prime time. Management asked the e-mail team to investigate cloud e-mail and after due diligence, the answer came back that:

- E-mail was not a commodity.
- Cloud e-mail services are not as mature as anticipated.

This led many organizations to scale back cloud e-mail plans."²

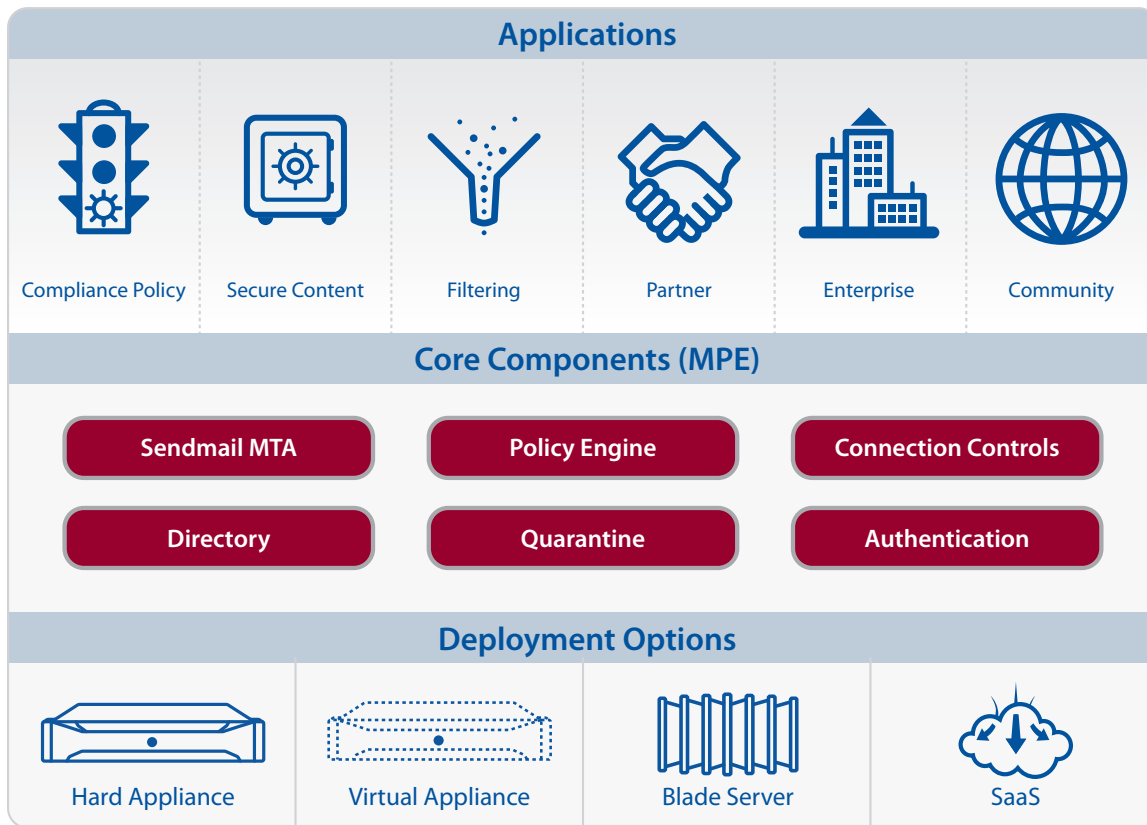
— Matthew W. Cain, Gartner

Even with pressure from IT executives to reduce costs by taking advantage of cloud computing, the messaging and security organizations for enterprises have discovered that doing so is not as simple as originally thought.

The promises of cloud computing can potentially be realized by migrating different layers of the messaging infrastructure to the cloud, and Sendmail has worked with many Fortune 1000 companies that have done so successfully. For those enterprises that have successfully outsourced messaging infrastructure to the cloud, virtually all of them have an on-premises email backbone layer based on Sendmail Sentrion Message Processors.³ The Sentrion Message Processors provide the critical internal email backbone infrastructure that glues all of the layers together.

Sentrion Message Processors

Sendmail Sentrion Message Processors are available in a number of different form factors and provide dozens of optional enterprise messaging applications (www.SentrionAppStore.com) giving businesses the power and flexibility needed to manage complex hybrid email infrastructure both in the cloud and on-premises.



Sendmail Messaging Architecture Review

A Sendmail Messaging Architecture Review is comprised of a thorough review and assessment involving input from the company's messaging team and other key business units. To support this, Sendmail Messaging Architects review the existing architecture and implementation, as well as current issues and concerns, to develop the following:



- Business objectives
- Short-term recommendations
- Long-term recommendations
- Recommended roadmap
- A comprehensive report and presentation are delivered to the organization for review and analysis.

Footnotes

1. Cloud E-Mail Growth: Slower than Expected, ID number G001172991, by Matthew W. Cain, November 2009
2. Cloud E-Mail Growth: Slower than Expected, ID number G001172991, by Matthew W. Cain, November 2009

About Sendmail, Inc

Sendmail provides appliance-based products, applications, and services that enable enterprises and government agencies to modernize their messaging infrastructures. Since 1982, thousands of commercial and open source customers around the globe have relied on Sendmail for a unified approach to the complex problems of policy-based message handling and routing. The company's comprehensive suite of applications addresses the challenges of gateway management, inbound threat protection, data leak prevention, email authentication, and intra-company message management. These applications run on the Sendmail family of Sentrion Message Processors, which are available in hard appliance, virtual appliance, and blade server configurations. Sendmail is headquartered in Emeryville, CA with sales and support offices throughout the Americas, Europe, and Asia.



Sendmail, Inc.

6475 Christie Avenue, Suite 350, Emeryville, CA 94608 USA

Tel: +1-888-594-3150 | Fax: +1-510-594-5429

Email: info@sendmail.com

www.sendmail.com

Copyright © 1998-2010 Sendmail, Inc. All Rights Reserved. All other company and product names may be trademarks or registered trademarks of their respective organizations. WP-01-0410