



**A Messaging Fabric:  
The Case for a Messaging  
Infrastructure Layer  
(v1.0)**

**Internet Research Group  
October 2010**

**About The Internet Research Group**

[www.irg-intl.com](http://www.irg-intl.com)

The Internet Research Group (IRG) provides market research and market strategy services to product and service vendors. IRG services combine the formidable and unique experience and perspective of the two principals: John Katsaros and Peter Christy, each an experienced industry veteran. The overarching mission of IRG is to help clients make faster and better decisions about product strategy, market entry, and market development. Katsaros and Christy published a book on high tech business strategy *Getting It Right the First Time* – Praeger, 2005 [www.gettingitrightthefirsttime.com](http://www.gettingitrightthefirsttime.com).



## Table of Contents

1.	Introduction and Overview .....	1
2.	Messaging Fabric Market Segment .....	2
3.	Messaging Fabric Benefits.....	3
4.	Basic Email Architecture .....	4
5.	Messaging Fabric Architecture .....	6
6.	Technical Capabilities of an Email Infrastructure .....	8
7.	The Advantages of Using a Purpose-Engineered and Supported Product .....	9
8.	Microsoft Exchange .....	11
9.	Messaging Fabric Rules .....	13
10.	Use Cases and Drivers .....	14
11.	Regulatory Compliance and IT Security .....	16
12.	The Increased Use of Email within Applications .....	17
13.	An Increased Desire to View Customers in a Holistic Manner .....	18
14.	An Increased Desire for Organizational Flexibility .....	18
15.	An Increased Set of Email Implementation Alternatives.....	19
16.	Summary and Conclusion.....	21



# 1. Introduction and Overview

Email was the first “Internet” application and in many regards is still the most important. A remarkable percentage of the general population reads and writes email every day. Email plays an essential role in the operation of most businesses and organizations. The volume of email traffic is huge by itself, and then amplified more than ten times with spam.

Ten years ago, an enterprise email system was relatively simple compared to today, with the primary requirement being the efficient and reliable delivery of messages within the business and with individuals outside. Today email is a much more important element of how we do business so the volume of messages and the requirements for reliable and timely development are all increased. More importantly, the issues of email security and regulatory compliance have changed quite dramatically and continue to evolve apace.

Not surprisingly, there is a good deal of specialized mail infrastructure that makes all this work behind the scenes. In this report, we have examined the need for a formalized messaging infrastructure in large enterprises, focusing on the use cases and value propositions today, while considering how external changes are driving this application segment in the future.

Our conclusion is that this is an important emerging product area and an important consideration for large enterprise, especially considering the business-critical importance of email, the compounding impact of regulatory compliance and security, and the value of preserving an agile email system that can respond quickly both to structural changes (e.g., acquisitions, divestitures and partnerships), as well as changing external demands (e.g., regulatory compliance and security).

This is a confusing market space for two specific reasons:

1. In smaller-- scale mail systems (e.g., SMB use) the capabilities in Microsoft’s Exchange offering provide useful solutions for many customers (for large-enterprise mail systems, the issue is the design and market center for Exchange and whether a product targeted at this market scales well into these much larger configurations); and
2. Historically Messaging Fabric solutions have been crafted from open-source offerings like Sendmail and the derivatives rather than being acquired as products. Compared to purpose-engineered product solution, the hand-crafted solutions are typically more costly (when the support of the custom offering is considered) and more complex given the incremental efficiency of a carefully

crafted product.

Sendmail Inc. has led the creation of products specifically for these solutions – the Sentrion appliances – by packaging their software offering (originally derived from the open source) into a high-performance, purpose-built appliance that can be configured, deployed and supported much more simply than a locally-constructed alternative (the product version has great benefit as the complexity and throughput of the solutions increase). We’ve chosen to speak of this new product category as a “Messaging Fabric” although “messaging infrastructure” would be more recognizable, to speak of explicitly engineered and supported solutions.

## 2. Messaging Fabric Market Segment

Much of this report is about the evolving requirements for a Messaging Fabric, but that is only half the story. The other half is the emergence of purpose-engineered high-performance Messaging Fabric products as an alternative to the solutions that have historically been crafted using open-source MTA offerings including Sendmail and its various descendants.

It’s hard to even imagine how much technology has evolved since Sendmail was first created, not to mention how much mail volume and processing complexity have increased as well. Early on, most MTA applications required only the capacity of an old server. But as time has progressed, message processing has gone from a not-very-demanding application on an old server to an application that can productively use every ounce of power in a modern multi-core CPU with a large RAM memory.

Sendmail Inc., Proofpoint and Cisco/IronPort have all demonstrated the differentiated performance of a purpose-engineered messaging appliance where the MTA code has been extensively rewritten to take advantage of modern server technology. To date, Proofpoint and IronPort have aimed these purpose-engineered appliances primarily at email security applications (e.g., spam mitigation). Sendmail Inc. uniquely has implemented a complete Messaging Fabric solution.

The market segment for Messaging Fabric solutions consists of:

- Microsoft Exchange (SMB solutions).
- Custom solutions often constructed from open-source pieces.
- Sendmail’s Sentrion appliance solutions.

Our examination of today’s offerings leads us to the conclusion that there is unique and differentiated value in the Sendmail Sentrion solution for large and complex Messaging Fabric solutions, and that this value is growing as mail volume and processing complexity continue to grow unabated.

These alternatives and the relative merits are discussed further in this report.

## 3. Messaging Fabric Benefits

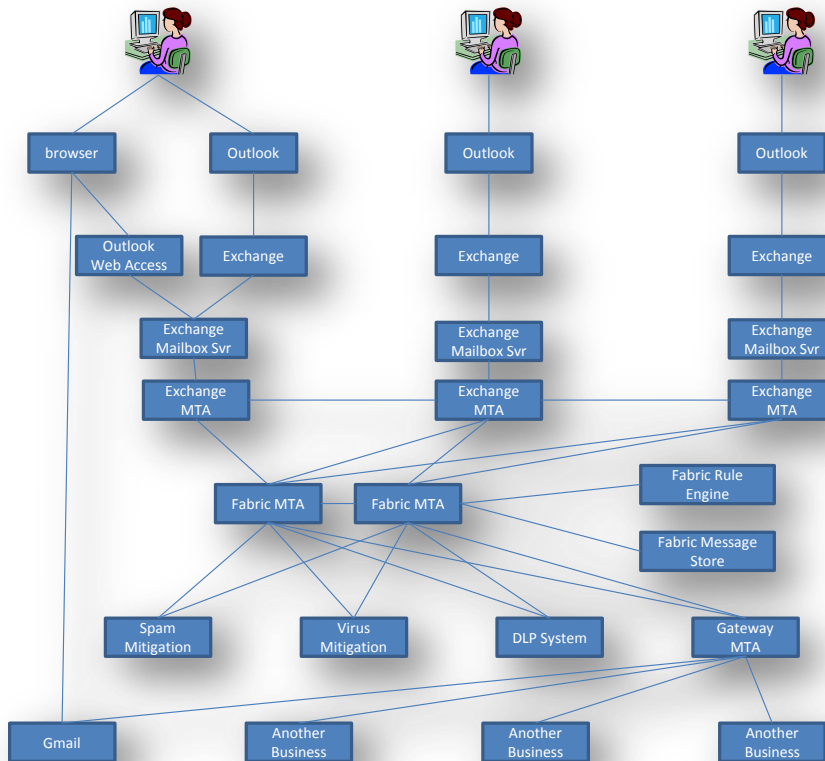
Having a formalized, purpose-engineered and supported Messaging Fabric brings these benefits:

- **Flexibility:** Formalizing the messaging infrastructure simplifies changing mail processing flows or adding new elements (e.g., new malware capabilities, simplified email upgrades, implementing new business functions such as specialized routing for help desk applications, or improved archiving).
- **Agility:** Having a flexible-messaging infrastructure enables relatively rapid changes to the email system, for example as a method of responding rapidly to organization change or acquisitions.
- **Scalability:** A flexible-messaging infrastructure makes it simpler to change the mail processing, for example as a means of dealing with ever-growing mail volumes.
- **Efficiency:** In many cases a flexible-message infrastructure can make the overall mail system significantly more efficient, for example by being able to triage spam messages as soon as possible.
- **Implementing mail enabled applications:** Today most enterprise business applications use email as part of the workflow (such as SAP or Salesforce.com) and a Messaging Fabric is useful for providing a larger framework which can apply policies and proper message handling.
- **Compliance:** Implementing activities which improve a company's ability to implement actions meant to conform to government regulations.
- **Reputation:** Through monitoring of outbound email, assuring that a company's email reputation is preserved and the company's mail servers are not subjected to blacklisting.

Our research concludes that there is real value in having a Messaging Fabric – a formalized layer of messaging middleware – above and beyond what is found in an email product such as Microsoft Exchange, and that this value increases rapidly as a large enterprise increases in size and complexity increases due to a set of external forces.

## 4. Basic Email Architecture

Most of us think of email through the lens of the software we use to read or write messages. At work many use Microsoft Outlook. At home many individuals read mail through a Web interface using a Cloud-based service (e.g., Google mail or Hotmail). In the last few years, smart phones are increasingly used to access email while mobile (e.g., Blackberry or iPhone).



These mail clients in turn connect to the application systems that provide mailbox services (storing and organizing received and incoming messages). In business, use of Microsoft Exchange Server dominates. Google Gmail and Hotmail are examples of very large-scale Web systems that provide mailboxes as a “Cloud” service. Technology suppliers like Openwave or Bizanga provide mailbox system components for service providers.

Mail Transfer Agents (MTA’s) are the system elements that understand how to transfer messages to another MTA via a network connection. In an enterprise, MTA’s connected to the Internet are the means by which messages to other organizations are sent and received. MTA’s are also used with a large messaging system to send messages between geographically distributed message stores.

Mail processing applications are the additional functions that are always needed

to implement a large mail system. They include **security applications** to triage spam from useful mail and to detect and block malware sent via email, **archiving applications** that are used for the long-term storage of mail as often dictated by regulatory requirements, and mail **content analysis applications** that are used to detect mail that invokes additional compliance requirements (e.g., mail with personal private information that must be encrypted when sent externally).

Email messages are sent between mail systems over network connections using Simple Mail Transport Protocol (SMTP) one of the oldest Internet application protocols. Mail destined for a particular address is directed to a specific mail system by resolving the domain name using Domain Name Services (DNS). The sending mail server connects to the destination mail server and then sends the messages over that link.

Messaging systems use other components of internal and external infrastructure:

- Directory systems such as Microsoft's Active Directory or LDAP: The directory is typically the authoritative source of information about the job an employee does, the organization they work in, and their work location.
- Internet and external Domain Name Services functions: DNS is part of the core Internet infrastructure, consisting of a set of directory resources that translate between human-understandable domain names (e.g., irg-intl.com) and (for example) the network address (the IP number) of the mail server that receives mail for that domain.
- Other Internet resources: Shared information systems play an ever increasing role in mail processing, for example, systems that gather data and assess the trustworthiness of various email servers based on their history of sending spam or maintain lists of computers that seem to be acting as part of bot networks.

## 5. Messaging Fabric Architecture

The Messaging Fabric is a middleware layer that integrates the components of a large, modern enterprise email system:

- The MTA servers that transfer messages between the various components internally and communicate externally with other mail systems.
- The mailbox servers that provide users access to their mailboxes.
- The various other analysis, transformation and storage systems required for security and regulatory compliance.
- The various other business applications that make use of email services.

For large enterprises, the infrastructure middleware can become substantial and serves a variety of purposes (all of which will be discussed in more detail later):

- A means of integrating malware services (e.g., spam and virus protection),
- A means of integrating a technically heterogeneous set of mailbox servers (e.g., Lotus Notes and Exchange or multiple vintages of Exchange).
- A means of integrating an organizationally heterogeneous set of mailbox servers (e.g., as the result of a merger or acquisition).
- A means of implementing content analysis applications in support of regulatory requirements and the mail transformation services required (e.g., the need to detect mail messages with sensitive data and encrypt them; creating a “Chinese Wall” between internal organizations).
- A means of integrating mail archiving services.
- A means of implementing message processing services delivery from the network (e.g., spam filtering done “in the Cloud.”).
- Providing a structure to integrate cloud services (such as Salesforce.com or Gmail) with in-house systems while simultaneously assuring proper message routing.
- A means of establishing and implementing corporate policies for scanning incoming and outgoing messages.
- A means of integrating email-enabled applications.
- A means of tracking email for administrative purposes (such as finding “lost” messages).

Technically we could use a Messaging Fabric layer to integrate these components in an arbitrary way. Practical email systems are structured with a standard layering of functions.

1. The mailbox servers form the “top” layer in the application architecture.

Within most enterprise IT architectures, these systems have grown into part of the collaboration system structure by which teams share information (Microsoft Exchange and SharePoint accessed via Outlook, for example).

2. A middleware layer – what most would think of as the “fabric.”
3. A gateway layer at the enterprise Internet boundary – Some security functions necessarily exist on the outer service (no one would put their Exchange mailbox or SharePoint servers in the network “DMZ” directly exposed to attack from the Internet). More importantly and perhaps less obvious, it is critical to perform basic spam triage at this level. Spam messages now constitute well in excess of 90% of the external mail stream. Fortunately, mitigation systems exist that can identify and block the majority of the spam traffic, in many cases without even examining the message content (because of the reputation of the sending server, for example). The practical network bandwidth, storage and processing savings that accrue if this is done before those messages enter into the middleware fabric are so great they practically dictate this kind of layering of application functions.

## 6. Technical Capabilities of an Email Infrastructure

Email messages and mail transmission are both very simple: messages are blocks of text data with some identified special (“header”) fields; messages are transferred to another mail system using SMTP, an equally simple protocol. Some headers are created when the message is created; others can be added or rewritten along the way; and others can be used to record the route by which the message was received (which other mail processors were involved along the way). Headers can be used to annotate the message (e.g., it has been scanned for spam or viruses).

The technical requirements for Messaging Fabric for a large company are also relatively simple:

1. **Throughput:** Obviously you have to keep up with the mail traffic, amplified by the huge volume of spam that has to be dealt with at some point (for many companies spam now constitutes more than 90% of the incoming messages, 10X the legitimate traffic).
2. **Robustness:** The probability of a message being lost must be very small. Software or component hardware failures aren’t an excuse.
3. **Flexibility and Control:** An ideal mail infrastructure system enables arbitrary choice and sequencing and control of a diverse set of processing functions, potentially from multiple vendors.
4. **Efficiency:** Given the large volume of messages, the processing and storage required can be substantial. More efficient solutions can have tangible cost of ownership benefits.

## 7. The Advantages of Using a Purpose-Engineered and Supported Product

Historically, Messaging Fabric infrastructure has been custom built for a large enterprise, by an email integrator or by IT, using open-source MTA technology such as Sendmail or its later derivatives. As discussed earlier, when Sendmail was first developed, it wasn't a very demanding application given the mail volumes and processing requirements of the time.

Since about 2004 (when spam grew to be the majority of mail volume) mail volumes have grown exponentially (driven by spam). Keeping up with spam and other email-born security threats has increased message processing requirements rapidly (although perhaps not as rapidly as email volumes have grown). Finally, regulatory compliance and broader security concerns (e.g., data loss prevention) have also increased the messaging processing requirements very substantially.

The net of all these changes is that message-processing systems are no longer simple or small applications. When IronPort created its first spam appliance, one of the engineering accomplishments was creating a "multi-threaded" MTA capable of taking full advantage of a single CPU so that the delays in processing for a message (e.g., waiting for communications protocols) could be optimized at the processor used on another message instead. Since that time, server CPU technology has evolved rapidly and inexpensive servers now feature multiple CPU parts (multiple "sockets") and each CPU has multiple cores (independent processors) with each processor capable of running in turn of executing multiple threads, all complemented by previously inconceivable amounts of RAM memory. On-balance servers are keeping up with Messaging Fabric processing requirements, but in a way that poses very significant engineering challenges. If you tried to run the legacy Sendmail open-source product on a modern server it would only use a tiny fraction of the available power. The net of all this is to acknowledge the value contributed by a product company (such as Sendmail Inc.) dedicated to evolving their product (Sentrion) to take advantage of the evolution in technology compared to either not doing that adaptation, or having that work done repeatedly by integrators on each deployment.

The first basic advantage of using a purpose-engineered product is to gain the benefit of an engineering team dedicated to keeping up with the application requirements and server technology. The second advantage has to do with complexity and scale. Suppose that a purpose-engineered and optimized solution is 50% more efficient than the alternative (can get twice the work done, a very conservative estimate given how rapidly everything is evolving). In the largest-scale use cases, more than one server is required, and all of a sudden the advantage is much more than a factor of two. As the number of systems increases, each system is less efficient due to the difficulties of load balancing and the need for coordination among the systems. So in these cases, faster is

really better.

Finally, an appliance solution such as Sendmail's Sentrion can also be performance characterized because the underlying hardware implementation is specified and the product can be tested against this characterization much more easily than with a software implementation that may run again on a diverse set of different server configurations.

To summarize, given the rapid progress in server cost/performance for many applications, performance optimization is of diminishing concern; but this isn't the case for messaging where message volumes have increased dramatically as have the per-message processing requirements. The largest messaging applications require carefully engineered solutions that get the most out of a modern server (a challenging and evolving task), both for simple efficiency and in order to minimize the complexity of the largest applications that require multiple servers. All of this demonstrates the value in a purpose-engineering solution compared to custom-integrated solutions, especially those built on open-source functionality.

## 8. Microsoft Exchange

Microsoft Exchange is by far the most commonly purchased email system and leads in installed mail seats as well. Exchange began as a departmental mail server, but has evolved over time to scale to “enterprise” class (aided by the amazing improvements in server performance and storage capacity), and has been functionally enhanced to implement a more complete set of enterprise email solutions. With the last two releases of Exchange (2007 and 2010), Microsoft Exchange has significantly improved the Messaging Fabric capabilities. It’s valuable to review these additions because they validate the importance of Messaging Fabric functionality, although we don’t believe this is the right basis for implementing the most complex Messaging Fabrics required as we will argue later in this section:

- **Multiple server personalities (“roles”):** The Exchange Server configuration can be specialized to perform transport functions, either as an Edge server (one that connects externally) or as a Hub server (one that connects internally). These server roles make it possible to expose the full mail flow for analysis (rather than just incoming and outgoing external email). The Edge role was designed to minimize the security “surface area” thereby hardening the system for operation in the network “DMZ.”
- **Microsoft’s continuing investment in security and email technologies:** Microsoft has continued to invest in a broad spectrum of email related technology: Malware detection and mitigation, spam mitigation, email archiving, data loss prevention (DLP).
- **The increased use of Active Directory:** Microsoft required the integrated use of Active Directory starting with Exchange 2000, and along with the increasing market share of Exchange, this helped establish Active Directory’s position today as the authoritative organizational directory in a high majority of enterprises. Integration with Active Directory enables Microsoft to offer more comprehensive Mail Fabric implementations since the organizational structure is an important factor in how mail is routed and processed.
- **Exchange transport rules:** Microsoft introduced and then has evolved a set of rule predicates and an engine for executing sets of rules in both the Hub and Edge server roles. Use of these rules permits a reasonably wide spectrum of mail analysis and transformation options, including rewriting elements of an email message or redirecting the message to a new recipient.

We believe that Microsoft Exchange can and will form the basis for Messaging Fabric solutions within the core SMB markets that Microsoft serves, but that large enterprises are much better served with purpose-built solutions. Microsoft’s great strength is taking complex software (such as Exchange) and engineering and packaging it so it can be sold at a disruptively low price with low attendant operational and support costs (compared to the existing solutions

that they displace). But Microsoft is happy to leave segments of the market to partners. The best example of this is the Citrix/Microsoft relationship in which Citrix builds on the basic Terminal Services offering and provides the most complex and demanding whole-product solutions while leaving the bulk of the market to Microsoft (over time Microsoft improves Terminal Services, but Citrix keeps moving forward and maintaining important differentiation). Microsoft's overarching goal is to increase the share of mailbox seats served by Exchange, and Microsoft will continue to add functionality to Exchange to address these broad market requirements. But it is not obviously in Microsoft's best interest to expend resources on the requirements of the most complex email configurations rather than expending those development resources on functionality that serve a broader market.

## 9. Messaging Fabric Rules

Beyond meeting these technical requirements, key features of Messaging Fabric systems are the rules by which messages trigger processing and the functions that can be specified, as well as the clarity and generality by which they are specified. Some of the important aspects of the Rule definitions and engine are these:

1. **Flexibility in predicate choice:** There are many logical conditions that might be used to trigger a rule (message content, message sender or any other function of the message header fields, the mail server or any attribute of the mail server, the sender or recipient and any attribute about their organizational position or roll.)
2. **Clarity of specification:** It's hard enough to specify logically what a rule should be, and harder still to do so in a way that is clear to others. Not only is it important that the rule logic be clear (the conditions under which the rule triggers), but also how the other rules are or are not examined when more than one rule triggers.
3. **Flexibility in how the processing is specified:** Similarly, it's important that the processing triggered by a rule be accurately specified in a clear manner.
4. **Vendor neutrality:** The rule engine should work with the broadest reasonable choice of other messaging components.

# 10. Use Cases and Drivers

Let's outline the drivers first and then discuss them in more detail as use cases. Simplistically, this is what is driving increased email importance and complexity that in turn increases the value and utility of having a well-structured Messaging Fabric:

- **The increasing volume and value of cybercrime:** Cybercrime is a big business and growing bigger all the time. For reasons we won't detail here, email plays an important role in this ecology (e.g., email delivers the malware that in turn creates zombie machines that are then used for high-volume spam delivery or DDoS attacks). Unfortunately, malware mitigation is a cat-and-mouse game of thrusts and counterthrusts. An effective and up-to-date system for email mal-ware protection is essential.
- **The increasing requirement of regulatory compliance and information security:** As IT assets become more valuable and more essential, they understandably receive more scrutiny. Almost all large businesses are subject to various regulations as publicly-traded companies, and as companies that harbor diverse private information and valuable business information. Since email crosses the boundary of the company, regulation often dictates specific requirements with regard to sensitive information contained in external email (don't send it, or at least encrypt it). The formalization of a Messaging Fabric allows the establishment of a single set of policies as opposed to a set of policy engines from different systems.
- **The increasing use of email within applications:** Today it is increasingly likely that all employees of a company will have email addresses (including those who don't use computers on a regular basis) and it is increasingly likely that an individual will have one or more personal email accounts and read email from those personal accounts regularly. The existence of large email services providing free accounts (Gmail, Yahoo, AOL and Hotmail for example) and the increased use of cell phones capable of receiving and sending email messages via these services, are major contributing factors in the rapidly growing use of email as a means of communicating with businesses. As email use becomes ubiquitous within a particular group, it makes sense that business processes and the applications that support and automate those business processes will increasingly use email messages as an important means of communication.

- **An increasing desire to treat customers in a holistic matter (“Customer Relationship Management”):** Over the last ten years, as more and more business processes were supported by applications, and as a growing percentage of the financial and operational records were stored in on-line data repositories, it was seen as increasingly important to aggregate all the information concerning a specific customer so it could be considered together, and to provide this kind of “360° view of the customer” in real time so it could be used as context during interactions with the customer.
- **An increasing desire for organizational flexibility:** Modern management dogma emphasizes focusing on core capabilities and being willing to sell-off and outsource secondary (non-differentiating) capabilities. For these reasons, and for other financial optimization purposes, large enterprises often have an ongoing divestiture, merger and acquisition stream. A Messaging Fabric provides a convenient way to adapt the email system to these changes appropriately with minimal disruption.
- **An increasing set of email implementation alternatives:** Many different factors have all contributed to the rapid evolution in “Cloud” services that offer new alternatives for the delivery of IT broadly and email-related functions specifically. For some time, basic spam filtering has been offered as a Cloud (delivered from the network service). Increasingly, email archiving or even mailboxes are provided as Cloud services. A Messaging Fabric provides the means by which a business can flexibly and agilely adapt their email architecture to take advantage of this growing set of Cloud delivered services.
- **Implementing backup and disaster recovery systems:** Planning for system availability and recovering mailbox access after an outage is simplified with the availability of a Messaging Fabric.

# 11. Regulatory Compliance and IT Security

Roughly ten years ago, government regulation started to cast a larger shadow on enterprise IT. A few verticals already were under reasonably stringent controls (e.g., brokers), but the introduction of the Sarbanes-Oxley legislation, the growth of credit-card processing regulation (PCI) and an increasing number of state regulations dealing with the disclosure of personal information, brought some form of regulation to a much larger collection of companies.

Like almost all technology, email is a double-edged sword: the convenience and immediacy that make email so valuable for improving business communications also make it very easy to inadvertently send sensitive material via email. Fortunately, it is possible to filter messages for sensitive content with reasonable efficiency and accuracy, and by doing so, be able to identify messages that contain what might generically be sensitive information (e.g., numbers that could be valid SS numbers or credit card numbers) or specifically are sensitive information (e.g., elements of names of known patients, known personal addresses).

The organizational position and role of the intended recipients of an email message can also be used to filter for inappropriate actions. For example, an email message sent to a group of senior executives that is now being forwarded outside of the company could easily be considered suspicious; mail sent to a large distribution list that included outsiders might be considered significant enough to hold the message temporarily and query the sender as to whether they understood the consequences. In the case of the HIPAA medical information regulations, sensitive data must always be encrypted when sent over the open Internet – identified sensitive messages can be diverted to a Web-based email system that enforces encrypted (SSL) access, while a conventional mail message is sent to the original recipient informing them that encrypted mail is waiting for them and telling them how to access it.

Having a Messaging Fabric makes it easier to keep up with (and to provide proof for compliance auditors) the evolving regulatory landscape, and to incorporate innovative methods of identifying and managing sensitive messages as they are found.

# 12. **The Increased Use of Email within Applications**

One of John Chambers' wise observations about the use of enterprise applications is that you only reap the full benefits of an automated process when you stop using the old process, as long as you have to run the new and old in parallel, it's hard to break even, much less save money. Email delivery of information has great potential benefits for creating such automated processes. For example, when all employees can be reached reliably by email then email communications can fully replace paper or postal mail communications and a great savings in cost and a great improvement in efficiency (e.g., as a means of making sure all employees are informed that now is when they can change their benefit plan). The same observation applies to commercial businesses dealing with their customers: there can be very significant savings improvements as well as effectiveness and efficiency improvements possible when email communication can be substituted for other forms (e.g., paper sent by postal mail). This is finally becoming possible in the last few years because of the availability of large-scale, very low-cost (or even free) email services (e.g., Google Mail, Yahoo, AOL or Hotmail), because of browser access to Web systems, and because of the rapid increase in the use of "smart" phones that are capable of reading and creating email messages.

Having a Messaging Fabric has many benefits when it comes to enabling and managing the use of email within applications:

- Enforcing the uniformity in these automated email mailings including assuring the use of up-to-date addresses, assuring that the individual is still suitable (e.g., still a business partner), and providing uniform logging, indexing and archiving of the mail sent.
- Providing flexibility in the use of external mail-related services (e.g., Cloud-based mail services for employees other than information workers).
- Providing the ability to organize and analyze all messages sent to and received from a particular organization, individual or other group.

## 13. **An Increased Desire to View Customers in a Holistic Manner**

Understanding your complete relationship with a customer – Customer Relationship Management (“CRM”) – has become increasingly important over the last decade, catalyzed by the increasing amount of information available from the various business process applications in use. The basic idea behind CRM is simple – make sure you orchestrate your relationship with a customer thoughtfully based on all aspects ranging from executive-level initiatives to specific product support issues. Obviously email is an important component of a customer relationship. Having a Messaging Fabric greatly simplifies the archiving and analysis of all relevant email communication, and provides unified access to this information for CRM purposes. Similarly, support help desks have specialized needs such as sending email with an embedded case number so that when the customer replies back, a different agent can continue handling the case.

## 14. **An Increased Desire for Organizational Flexibility**

As email plays an increasingly important role in how a business or organization operates it's obviously important that the email system doesn't constrain organizational flexibility or agility. Dealing with changes can be no small challenge given, for example, the task of integrating email systems after an acquisition or (to a lesser degree) after a major reorganization.

Having a Messaging Fabric can be a highly valuable tool in these circumstances since it provides a convenient way of rewriting mail headers on the fly as a way of adjusting to change during the time it takes the change to be adopted more broadly (e.g., a new company name and email addressing format being accommodated in all the email sent to the company).

# 15. An Increased Set of Email Implementation Alternatives

For a very mature application, there is an amazing amount of ongoing change to email and email use reflecting both the continuing increase in mail volumes and spam and the evolving processing alternatives such as Cloud-based mail elements. Having a Messaging Fabric makes it much easier to evolve an organizations' messaging system while minimizing disruption. Examples of drivers in this area include the following:

- **The availability of Cloud-based spam filtering services:** Starting some time ago, mail filtering in the Cloud (as a network access service) became possible. Cloud-based filtering is attractive because a good deal of spam can be confidently blocked with little specific inspection of the message (e.g., based on the reputation of the server sending the message), and doing so frees up incoming bandwidth since 50% or more of the message traffic had been blocked before it even showed up.
- **The availability of Cloud-based messaging archiving service:** As regulatory compliance requirements have increased, more and more organizations have a legal or governmental responsibility for preserving messages for multiple years in a robust manner. Since an essential part of robust messaging archiving is some form of reliable offsite storage, there is an elegance and simplicity to using a Cloud service rather than building an in-house implementation.
- **The availability of Cloud-based mailbox systems:** In the last five years, reliable and relatively inexpensive (compared to running a conventional in-house systems) mailbox systems have become available (e.g., Gmail or hosted Microsoft Exchange). These systems are particularly attractive as a means of providing mailboxes for employees who would otherwise not need access to information applications (e.g., workers in service industries such as fast food).
- **The availability of specialized email processing appliances:** As message volumes and rates have increased it has been necessary to greatly scale elements of the mail system, and has led to the availability of specialized messaging appliances (e.g., for elements of security) that have been purpose-engineered for maximal efficiency and throughput. A flexible Messaging Fabric layer makes it much easier to take advantage of these new systems as they become available in a minimally disruptive fashion.
- **The alternative of running email system elements on a virtual server fabric:** Data Center virtualization is one of the most visible IT initiatives today and provides incentives to move server applications onto a shared, virtualized data center system. Having a flexible Messaging Fabric makes it much easier to move selected message system elements into a virtualized implementation with minimal large-scale disruption.

- **The ability to use a Messaging Fabric as the basis of a gradual email upgrade (e.g., from Exchange 2007 to 2010):** Email system upgrades are important in order to get new functionality and often to cost-optimize the system, but are extremely disruptive both at the system and user level. A flexible Messaging Fabric provides a means of doing a more gradual email system upgrade which can be of great value to the messaging team both in terms of spreading out the work over time and spreading out user retraining.

# 16. **Summary and Conclusion**

The ever increasing message processing requirements at the core of the biggest email systems used by many of the largest enterprises have created a new product category which we have coined Messaging Fabric solutions, pioneered by Sendmail with its Sentrion appliance solutions. Although standard mail offerings such as Exchange suffice in the SMB space, for these largest applications we find great value in purpose-engineered solutions in contrast to the custom solutions often based on open-source parts built by messaging integrators today.