



Reliable and Scalable Email Systems

Email's Evolution from Applications to Appliances

Executive Summary

Over the past ten years a fascinating trend has overtaken several areas of high-technology, and appears ready to disrupt numerous more: commonly used, complex software applications have shown a strong tendency to evolve into appliances - hardware and software bundled into a single package - dedicated to accomplishing the purpose of the original application. This trend has repeated itself many times; markets where this is best exemplified include firewalls, routing and encryption.

Why does this trend occur? These common applications, which start as software running on a general purpose operating system and server, evolve into hardware-based platforms for three basic reasons: security, performance and manageability/control. In addition to these key customer demands, a hardware solution provides other benefits including ease of deployment, configuration, and updating. The ease of deployment and maintenance also often outweigh the cost of installing a single purpose-built server in the data center, resulting in a lower cost of ownership (TCO).

So what industry will experience this trend next?

This white paper discusses why the appliance model is the logical next step for email, the provisioning, serving, storage, access and archiving of email accounts and messages. We'll examine the highly unreliable and insecure nature of legacy messaging applications that typically exist across enterprises (typically Microsoft Exchange or Lotus Domino), and show the advantages of moving toward hardened, secure messaging appliances. We'll discuss how the usage and security risks in software-based messaging environments - frequently the most critical data store and communications tool in any organization - compel the move to the appliance model as IT managers recognize how traditional software-based email systems are no longer the optimal messaging solution.

The Evolution of Email

Email usage has changed significantly over the years. Originally an obscure university utility perceived more as a novelty than business tool, email has evolved into a highly cost-effective, "always on" communication necessity for businesses everywhere. According to a recent report from analyst firm Gartner Group, 80% of the business executives surveyed believe email is more valuable than the telephone for business communications while 74% of respondents said it would be more of a hardship to be without email for five days than to be without the phone for that long. As this survey indicates, the way businesses communicate has changed. People are sharing information much more frequently and in vastly different ways than they did just 10 years ago. The work force is much more mobile than before. Users are constantly connected to the Internet, whether

at their desks or remotely, which has led to the skyrocketing popularity of mobile devices like Research In Motion's BlackBerry™ device or Apple's iPhone™

Major changes in electronic messaging today appear in the:

- Skyrocketing volume of messages - an average of 160 messages per organizational mailbox per day by 2009
- Growing size of messages (with file, picture, music, video, and other types of attachments)
- Increasing amount of sensitive content in emails (product orders, patient information, financial documents, etc.)

All these factors directly affect the performance, security, and manageability of the messaging network with IT departments struggling to simply address basic messaging needs. To make matters worse, legacy-messaging tools were not designed for or built to handle these changing conditions and thus have not kept up with these changing customer needs.

In addition, new requirements for email systems have appeared. Email's popularity has resulted in the proliferation of security risks like viruses, phishing and spam. The increased exchange of sensitive information through email requires additional security measures. The explosion of regulatory oversight requires companies to keep records of electronic communications for long periods of time and in a format and repository that support quick retrieval. Software messaging systems like Microsoft's Exchange Server were not built to cope with or adapt to these changes in email usage, and they fail to meet new standards for performance, flexibility, and security. For example, Exchange fails to support granular, per group/role/user policy enforcement required by today's demanding messaging environment. And Exchange's software architecture requires a Windows operating system (OS) that treats security as an afterthought, leaving the entire messaging network vulnerable to hackers and malware writers.

What is needed is an easier, more reliable and safer system for handling messages.

Common Dilemmas and New Requirements

Many companies start with several general-purpose servers running Microsoft's Windows operating system to support their initial messaging, business applications, and human resource needs. However, as many of these companies soon realize such a framework is neither robust nor secure enough for the demands being placed on a typical message network today. Even normal operation of such a framework is plagued by high costs, poor performance and dismal reliability - requiring specialized personnel to manage the messaging application. Worse yet, when a company's employee population or business needs increase to the point where the original servers can no longer support the company's requirements, the tendency is to add more servers and more software licenses, which simply exacerbates matters by creating an even larger and more complex array of subsystems that are a nightmare to administer and secure.

When you add the heavy usage, large files, virus filtering, spam filtering, and content filtering that are integral parts of today's email systems, performance is severely taxed in a traditional software-based environment. Security alone is a continually escalating battle, due to vulnerable general-purpose operating systems like Windows, which must be patched on an alarmingly frequent basis to prevent exploitation. How much of a concern should the integrity of a Windows-based system be? One study found that an unprotected and unpatched Windows XP system lasted only 4 minutes on the Internet before it was compromised

Many large enterprises utilize email software such as Microsoft Exchange, Novell GroupWise, or Lotus Notes/Domino to handle email, calendaring, tasks and other functions. They dedicate servers to handle SMTP, POP, IMAP and LDAP tasks, which are typically nothing more sophisticated than Intel or AMD boxes running Windows applications. The result of this data center setup is a mission critical application - email - running on a general operating system running on general purpose hardware. Because the Exchange or Domino application only addresses the enterprise's email and collaboration needs, the enterprise is forced to deploy separate "point solutions" to address their other messaging infrastructure needs - like security, storage, archiving, and policy enforcement. Because these point solutions have generally grown up from much smaller systems with fewer requirements, the enterprise's email network now consists of a hodgepodge of often poorly integrated directory, storage, mail, security, and policy "solutions." Each point solution usually comes from a different vendor with different hardware and software infrastructure requirements that must be separately managed, updated and maintained. As a result, expensive specialists are needed to run the disparate systems. Furthermore, applications that aren't built to work together have "gaps" between them: the applications do not take advantage of hardware or software architectural features to speed performance or to minimize security gaps that can be exploited by malware writers. And since the systems are on separate computers, there are no cost savings from integration.

Another shortcoming of this approach is that the email or IT administrator is required to call a different support number in case a system experiences a problem or they have a question. Worse yet is the seemingly ridiculous struggle of obtaining agreement from various vendors about whose system is actually at fault when downtime does occur; according to a recent study from Osterman Research, troubleshooting email problems costs twice as much as the downtime from such problems!

All of this makes the email or IT administrator's job very difficult. Two essential parts of the administrator's job description are to minimize downtime while lowering costs wherever possible, often by consolidating servers. Yet the severely taxed, compromised email systems used by most enterprises actually increase downtime thereby forcing administrators to use more and more hardware to cover up the problems rather than address the root cause.

Low TCO is not a realistic goal when the email system is based on separate application-based platforms. Due to the specialized nature of the numerous point applications, management and maintenance costs are high to begin with and grow exponentially as users are added. In addition, hardware costs escalate as network demand increases due to the performance shortcomings inherent to legacy application-based email systems.

In sum, a key shortcoming of software-based network, storage and security solutions is that they typically run on standard operating systems that are less reliable, more complex, and much less secure than hardened appliances dedicated to specific tasks. These problems are exacerbated when companies add more servers and more applications onto their initial systems as the companies grow and their needs change. Performance suffers, administration becomes more difficult, and costs skyrocket as the systems become more complex. This daunting situation created by legacy applications has been the primary driver behind the transition from implementing such applications as plain software running on standard servers to the utilization of appliances - purpose-built systems which are designed specifically to perform the tasks of those applications.

From Applications to Appliances

The appliance model offers a unique solution to the problem of a complex application with evolving requirements - like email. Appliances provide a proven model that transforms a collection of complicated, disarrayed applications into a single faster, simpler, more reliable, more secure device. The overwhelming majority of organizations already employ specialized appliances to handle functions such as firewalls, encryption, and routing, thus making the deployment of an email appliance a simple and logical extension of this approach.

In the past firewalls - used for isolating networks from each other, especially internal networks from the Internet - resided on generic computers and networks, requiring specialized IT attention because of their complexity to create and maintain. By contrast, today's purpose-built firewalls from companies like Juniper Networks, Cisco and Fortinet have replaced the traditional software-based firewalls in most enterprises. Data encryption - used for protecting data content regardless of the security of the route it travels - has also been offloaded to dedicated devices to free up CPU cycles and boost network performance. Routers - used for intelligently directing data traffic moved from general-purpose computers to separate appliances optimized for performance and security some time ago. All three of these transformations occurred because these technologies represented popular applications that needed better performance, tighter security, and easier installation, configuration, and updating.

Email Appliances

Email has become the ubiquitous communication tool for businesses of all types and sizes that require security, reliability, good performance, and support for legal compliance needs - all preferably at a reasonably low cost. It is thus logical to assume that this medium would evolve from a patchwork of disparate applications into appliance-based systems in order to meet customers' increasingly demanding messaging needs.

Email appliances that include most of this functionality surrounding a core email application have actually been available and meeting the needs of customers for the past seven years. They:

- Handle end-to-end email security, including anti-spam and anti-virus protection, and user and sender authentication
- Are powered by a hardened OS with no known exploits
- Greatly enhance the user experience through vastly improved uptime reliability and simple scalability of the messaging network
- Enable granular policy requisition and enforcement for managing groups, roles, and users across heterogeneous user bases and geographies

Unlike software applications like Microsoft Exchange and Lotus Domino that require setting up servers with the appropriate infrastructure and then installing the email software, these messaging appliances can be deployed in minutes because they are intended to be "plug and play." The purpose-built messaging operating system on each device is hardened, which not only greatly reduces security vulnerabilities, but also has been tuned to improve performance. Since the appliance is dedicated to the

purpose of supporting a messaging system, parts of the hardware can also be built to cater to messaging-specific needs, such as having redundant power, hard drives, and memory to reduce downtime risk to an application for which uptime is critical. The operating system is built to work with the hardware and the messaging system in a single, unified "stack." Having the entire email system on a single box also reduces network traffic and improves delivery time, especially between internal users because the system is delivering messages between users with mailboxes on the same server the appliance essentially "owns" the entire SMTP network. An email system using appliances often can be scaled by simply adding more appliances – a clean and simple solution for growing with a company's needs. By combining the security and compliance needs of an email system into one device, an email appliance arguably reduces costs associated with management and maintenance, resulting in a significantly lower TCO.

One Solution for Multiple Email Challenges

Mirapoint's Message Server line of email appliances solves a broad range of messaging issues that confront every IT department. These include:

Secure messaging: First and foremost, everyone with an email system must defend against the growing amount of spam and constantly evolving viruses that threaten electronic communications. Mirapoint's Message Server provides multiple layers of spam and virus protection from the time a message reaches the edge of the network to its delivery, with a 98% overall catch rate with virtually no false positives. First, Mirapoint's Reputation Hurdle identifies common SPAM and malware senders, blocking their IP connection before they reach your email gateway. Next, Mirapoint Mail Hurdle technology blocks up to 80% of threats at the network edge by dropping non-RFC compliant connections before any system resources are used to evaluate individual messages. Then Mirapoint uses its proprietary Reputation Hurdle and RAPID Anti-Spam and Anti-Virus technology to analyze internet traffic patterns in real time to further filter out spam and viruses. Finally, Mirapoint employs Sophos and F-Secure anti-virus technology to scan messages before delivery.

Optimized email performance: General purpose systems fail to optimize performance because they are designed to accommodate so many different applications. These systems also include extraneous features that further degrade performance. By contrast, Mirapoint designs its appliances to maximize the economy and speed of the system's integrated messaging functionality. For example, Mirapoint's DirectAccess routing technology works directly with Web and wireless client interfaces without any gateways or translations, dramatically reducing response time, system overhead, and administrative resources.

End User Controls: Mirapoint's Junk Mail Manager easily handles the increasing amount of spam via individual quarantine mailboxes deployed on the edge security appliance. This unique approach reduces the load on the core mail server and network, thereby cost-effectively boosting overall performance and responsiveness of the email network. It also allows individual users to set their own spam thresholds via allow/deny lists and other granular controls, thereby offloading some of this time-intensive responsibility from the IT or email administrator.

Regulatory compliance: Mirapoint helps enterprises and financial and healthcare institutions comply with the likes of Sarbanes-Oxley, Graham-Leach-Bliley, HIPAA, Basel II and other government mandates. Centrally-managed, policy-based controls of outbound filters, as well as automatic routing and/or copying of messages to storage devices for audit or archival purposes help organizations meet compliance requirements while facilitating a rapid response in the event corporate communications are subpoenaed or otherwise needed. With this approach, regulatory compliance and global policy enforcement are ensured without relying on the diligence or subjective judgment of individuals.

Conclusion

Mirapoint has taken email to the next level - to the appliance model. Mirapoint has applied the lessons learned from other industries like firewalls, routing and encryption to take a leadership position in the provision of secure and scalable messaging solutions to enterprises, service providers, and government and educational institutions. Our primary goal is to make messaging simple, secure, reliable and cost effective. We'll help you build a secure messaging infrastructure from end-to-end and simplify the entire messaging architecture.

For more information on how Mirapoint can improve the security and service delivery of your message network, visit our Web site at www.mirapoint.com, or call us at +1-408-720-3700.

Mirapoint Software, Inc.

1215 Bordeaux Drive,
Sunnyvale, CA 94089 USA
Tel: 1-800-937-8118
Tel: +1-408-720-3700
Fax: +1-408-720-3725
Email: info@mirapoint.com
www.mirapoint.com

©2009 Mirapoint Software, Inc. All Rights Reserved. Mirapoint is a registered trademark and Mirapoint Reputation Hurdle and Mail Hurdle are trademarks of Mirapoint Software, Inc. All other trademarks are the property of their respective owners.