

The Message Processing Platform and Enterprises

January 2005



Email, the first major application of the Internet, has become part of the fabric of modern society and the bedrock of business communication. However virus, spam and other security risks threaten to destroy the viability of this essential communication medium.

The current email security environment is one in which old threats such as viruses, worms and Trojans have increased in volume; spam and phishing have transformed from minor annoyances to major problems. In addition, government regulations on data privacy and protection are increasing liability and driving spending. Regulations such as The Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) require institutions to keep a record of their email communications and secure confidentiality of information. Steep penalties can apply to those organizations that do not comply with their industry's regulations. The email security problem is no longer just viruses.

The email security threats, if unmitigated, may result in the following well-known risks:

- Confidentiality breaches
- Damage to reputation
- Lost productivity
- Increased network congestion and storage requirements
- Legal liability

These risks are creating opportunity in the marketplace. Email security has become a major area of investment attracting many venture capital firms. With so much capital and research flowing into the email security industry, innovation is taking shape. At the same time, the din of email security vendor claims makes it almost impossible to see the truth about the state of email security technology. It seems that every vendor captures 99% of spam with few to no false positives and that all of them leave you safe from any known email-based attack. However, the intelligent reader is not fooled by such marketing claims.

Many vendors provide point solutions that address part of the problem. Others will claim that their integrated solutions take care of all known problems. For example, many vendors offer all-in-one appliances that are typically deployed at the network perimeter. However, relying on an appliance-only solution is risky and large enterprises and service providers require more flexibility than is possible in an appliance.

On the other hand, server-based solutions better address archiving and content filtering and can prevent the internal proliferation of viruses or worms that infiltrate your network. However, a large organization can have tens, hundreds or even thousands of email servers and installing software on every email server can be a daunting and expensive task.

In contrast to these limited solutions, one's security architecture needs the following:

- Multiple deployment options
- Genetic diversity
- Customizability

Deployment options: For the ultimate in flexibility, email security needs to be deployed on multiple points, not just on a perimeter device or email server. The choice needs to be yours.

Genetic diversity: The experienced reader knows that relying on a single vendor for an end-to-end technology solution is risky. The best-of-breed approach can provide additional layers of protection that a single-vendor solution cannot provide. No software company can produce a panacea to all email ills and it is unwise to bet on a single vendor to protect your email system – no matter how nice their brochures may be.

Customizability: As with all technology solutions, technology companies struggle to provide the real-world industry expertise needed to tackle your business-level problems. It is quite simple to produce a nice brochure or website expounding on a company's expertise in an industry. No one knows your business needs better than you do, especially not a bunch of software engineers who have never worked a single day in your business or industry.

MPP Value Proposition

Businesses need forward-thinking tools with flexible deployment options to protect against present and future email threats. It is well known that having first entrant advantage does not confer market advantages. Today's leaders in email security may not necessarily be the leaders in protecting against tomorrow's threats.

The MPP enables forward-thinking security architectures by integrating comprehensive policy tools with embedded security and best-of-breed commercial and open-source technology. We integrate many popular email security packages and feature centralized quarantine and archiving databases and directory-based provisioning. Our technology may be deployed in multiple locations, in the right locations for your business needs.

Message Partners provides the integration and management tools you need to apply technology innovation to your unique business-level email problems. We don't provide a one-size-fits-all solution. But we do provide the ability to integrate best-of-breed email security technologies into a cohesive email security architecture that solves the security and compliance problems unique to your business.

The Message Processing Platform

Best of breed Integration

The MPP provides a policy framework, management, monitoring, archiving and the ability to mix and match any of our virus, spam, or content scanners. All of our services may be selectively applied on a per-domain or per-user basis and our directory integration allows policy membership to be stored in your existing LDAP user directory.

With the MPP, you can have a comprehensive email security policy that addresses viruses,

spam along with content. This policy may be implemented using LDAP, which provides flexibility and scalability.

We currently support scanning engines representing the best of commercial and open source technology. Unlike many email security vendors who are re-packaging open source solutions and doing their best to hide this, we are proud of our capability to blend open source and commercial technology to suit your business requirements.

We currently support four virus scanners: Sophos, F-PROT, Pattern Authority (Cybersoft) and Clam. F-PROT and Clam are integrated into most of our products and the others may be added to your environment in seconds.

We currently support three spam/fraud scanners: Cloudmark, Pattern Authority and SpamAssassin

We currently support Pattern Authority as a content scan engine. Pattern Authority has a powerful pattern-matching engine (CVDL) for custom pattern creation.

Archiving is supported using a file system or the popular MySQL database. By using a standards-based database, it is possible to build retrieval and analysis tools quickly and easily. We are not claiming to solve all archiving problems; however, our archiving solution is scalable and reliable and may be applied on a per-customer basis. Complete archiving solutions offer comprehensive retrieval and compliance analysis tools and we expect robust third-party activity in this space.

MPP Solution Offerings

There are three versions of the MPP targeted at different market segments. All engines are supported on all versions of MPP. MPP may be deployed Linux, Solaris, OS X and FreeBSD on Sendmail, Postfix, Qmail, CommuniGate Pro or SurgeMail email servers. Any of these servers may be SMTP gateways or production email servers.

The MPP SE (Standard Edition), formerly known as MPP 1.0 and MPP LE, is targeted to the SMB, Education and ISP markets. The MPP SE has limited policy control and supports all scan engines. The MPP SE supports virus, spam and limited content filtering. MPP SE has two virus scanners integrated and others may be optionally added.

The MPP Enterprise and Service Provider Editions add many features to MPP v1 including our directory-integrated policy engine, SNMP monitoring, basic archiving, content and harassment filtering and many “bells and whistles” that are a must for larger environments. MPP Enterprise is bundled with the innovative Cloudmark Authority anti-spam and anti-fraud scan engine.

MPP Markets

Enterprises, service providers, and education customers can use MPP. Here are some examples:

- Service providers or centralized technology organizations that need to offer different service levels to their business units or customers.
- Email service providers who wish to save years of development time to build a scalable email service offering.
- Enterprise customers who need to build scalable and flexible email security architectures that leverage open source and commercial technology.
- Customers who need to build standards based archival solutions. Our archival technology integrates with Illumin or you can build your own retrieval tools based on our open MySQL tables.
- SMB, ISP and Education customers who need server based email security services.
- Customers that need to deploy a centralized quarantine store with customizable end-user quarantine review. Our customizable quarantine interface may be used with any

of our engines, including Spam Assassin.

- Schools or businesses that need to deploy strict content filtering to comply with content standards.
- Enterprise customers who wish to offload journaling from their MS Exchange servers.

The MPP for Enterprises

Enterprises have the following requirements:

- Performance
- Reliability and Availability
- Scalability
- Manageability and Provisioning

Performance

The MPP is built on a multi-threaded core capable of extremely high-performance scanning. The MPP can scale to well over 50 messages per second, which is highly dependant on hardware, disk speed and choice of email server. The MPP is mostly disk-limited so using standard techniques for improving I/O rates will improve performance.

Performance will also be influenced by the choice of engines.

MPP uses persistent connections in the form of connection caching or pooling as a way to minimize CPU load for a number of key features. Connection pooling applies to the CommuniGate and Cybersoft Pattern Authority interfaces along with MySQL archiving. Other module interfaces create connections at each request as the setup is not CPU intensive.

Reliability and Availability

MPP uses high-performance scanners that have been used by major service providers and

enterprises for years. MPP supports constant scanning during signature reload for all scanners.

Scalability

MPP may be deployed on mail clusters, or hundreds or thousands of email servers in an organization. Our centralized policy administration and LDAP integration enables a consistent configuration across all MPP instances.

MPP is currently protecting over 1,000,000 email boxes with individual installations with hundreds of thousands of users.

Manageability and Provisioning

The MPP is controlled by an XML configuration file which can be configured via our server-based Webmin GUI or any popular text or standard XML editor.

MPP policy membership can be stored in your existing LDAP schema. And unlike some vendors who require you to populate every configuration option in your LDAP directory, we require minimal schema modifications. Our dynamic LDAP support enables fast synchronization between provisioning changes and service activation.

Your existing LDAP import tools will work.

Reporting tools: The MPP SNMP MIB is a completely standards-based tool to provide in-depth analysis of your email communication patterns including message rate and volume, virus, spam and error counts, top senders and receivers and more.

MPP SNMP data may be accessed via any standard SNMP polling application and reports can be generated using your favorite reporting tools.

Summary

There is no one-size-fits-all solution for the myriad of email security and compliance problems facing businesses. MPP provides the right solution by focusing on integrating embedded and best of breed commercial and open source tools to build forward-thinking, policy-driven email security.

About MessagePartners.com:

A leading provider of email security software, Message Partners provides email security and compliance solutions for business-critical email systems. We have been providing email security solutions since 2001.

Message Partners Inc.
271 North Avenue, Suite 1210
New Rochelle, NY 10801
(877) 302-2027
(914) 712-9050
(914) 206-9609 - Fax
info@messagepartners.com
AIM – RAEINTERNET