



Email Security Success: Securing your email infrastructure

What's been going wrong and how to fix it.

Securing your email infrastructure in 2007 what's been going wrong and how to fix it.

“ Current approaches to email security be they LAN or Managed Service Provider based, are failing to eliminate vulnerabilities. ”

“ Mimecast resolves the numerous problems inherent in current email security. ”

“ Within the SMTP protocol and the construction of an SMTP email message, there are several opportunities to exploit weaknesses. ”

“ Mimecast users avoid the cost, risk and embarrassment of lost messages without the need to apply administratively intense quarantine monitoring. ”

Email is now your most critical business application. It warrants robust protection. However, current approaches to email security be they LAN or Managed Service Provider based, are failing to eliminate vulnerabilities. Customers now face increased complexity, decreased control and visibility, variable effectiveness, noticeable message delivery delays and inadequate protection from new threats.

Mimecast ARMed SMTP is a unique next generation approach to email security. This whitepaper explains how Mimecast resolves the numerous problems inherent in current email security and how to combat the various new forms of email security threat that your network will probably be subjected to.

The anatomy of an email attack:

Email is a popular tool for criminals on the Internet. It is attractive to criminals because of the wide population of systems and users available to interact with on an almost entirely anonymous basis. Whether the attack is simply spam based or a complicated and directed blended-threat the intention is frequently financially motivated and the target is often random.

There are four general types of attack:

1. A **directed criminal attack** aimed at stealing information or compromising the systems of a specific company or network, often deployed using specifically crafted tools.
2. A **recruitment attack** aimed at extending the attackers own network of "zombies" or machines under their control which are subsequently used for hire or to deliver spam, propagate viruses and/or mount distributed denial of service (DDOS) attacks.
3. A **sabotage attack** aims to wreak havoc on an organization or the Internet in general. These are often ego motivated where the attacker or author of the virus seeks either vengeance on the victim, greater notoriety or financial gain, usually through blackmail.
4. A **spam/scam attack** aims to pump unsolicited commercial or fraudulent bulk email onto your network in the hope of either winning the custom of your staff, having them participate in a program that benefits the scammer (e.g.: buying a particular stock), or have them provide valuable information to the attacker. (e.g. Phishing)

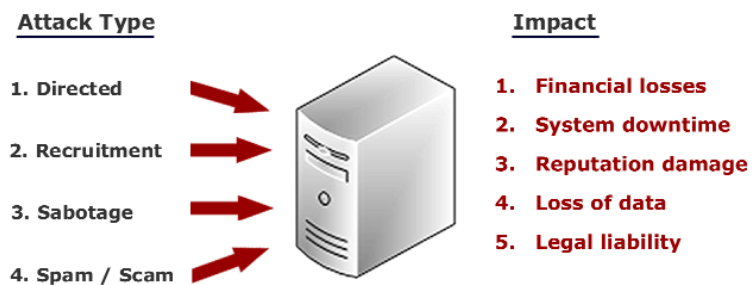
The anatomy of an email based attack, whether directed or spam based, will be determined by the intentions of the attacker. Within the SMTP protocol and the construction of an SMTP email message, there are several opportunities to exploit weaknesses both known and unknown. This allows the attacker malicious access to your resources.

“ An integrated blend of defensive techniques and intelligent counter measures are required. ”

“ With the advent of blended threats, the disciplines of virus/malware and spam fighting have begun to merge. ”

“ Companies are failing to provide comprehensive protection for their email systems. ”

“ Managed service providers offer clients shared use of large deployments of software originally designed for single company use. ”



The four attack types and threats presented.

An attack can be one or a combination of the following:

- a. An email attachment containing malicious executable code
- b. Encrypted content as above
- c. A file embedded inline in an email message
- d. The construction of the SMTP or MIME of the message itself
- e. HTML elements within the message or direct link to malicious websites
- f. An abusive delivery pattern aimed at stealing information or denying service to your networks

Malicious content can require the cooperation of the recipient to execute or seek to exploit a pre-existing vulnerability within the operating system or other software resident on the recipient's machine without the co-operation of the recipient. In many cases malicious code seeks to propagate itself and infect other machines using the resources of machines already compromised or those vulnerable to exploit.

To provide comprehensive protection against all types of attack an integrated blend of defensive techniques and intelligent counter measures are required.

A standard Anti-Virus signature scanning and content filtering approach, for example, may catch a large proportion of known attachment based sabotage attacks; however it will be helpless against a specific targeted attack or sabotage attack using a denial of service vector.

With the advent of blended threats, the disciplines of virus/malware and spam fighting have begun to merge to form a single email security discipline. Mimecast ARMed SMTP is a leading example of this discipline and delivers a new and more effective strategy for email security.

Why do we need a new approach to email security?

There are four primary factors making a new approach critical.

- 1. Companies are failing to provide comprehensive protection for their email systems on their own LANs without major tradeoffs in performance and manageability.
- 2. Managed service providers offer clients shared use of large deployments of software originally designed for single company use. This removes visibility and control from the client, fails at best-practice, and penalizes legitimate email delivery during attacks and peak usage periods.

“ Attacks targeting some of their customers will affect the processing and delivery of messages for all other customers sharing the same system. ”

3. Threats are evolving and becoming more severe as the financial rewards available for even moderately capable attackers grow.
4. The financial or compliance based penalties for not providing adequate levels of protection are now beginning to affect organizations, either through inflated management cost, insurance premiums or regulatory pressures.

Companies are failing on their LANs:

Despite the availability of so called 'best of breed' email gateway systems, many companies find that they still cannot cost effectively assemble and manage comprehensive and scalable email security and policy control on their own networks without introducing:

- Undesirable single points of failure within the email delivery path.
- Delivery performance degradation at peak usage times.
- Significant in-house technical expertise and administrative overhead.
- The constant risk of false positives which disrupt business communications.
- Complex systems with disparate management interfaces.
- Exposure to bandwidth loading on their WAN connections.

As a result of these shortcomings, many companies seek to augment their email infrastructure by using Managed Service Email Security Providers. These providers however face challenges of their own, that directly affect the end user.

Managed Service Providers are failing on the Internet:

Larger managed service providers are now responsible for delivering a fair volume of corporate email traffic.

They are also responsible for the significant slow down in the delivery of legitimate business emails over the second half of 2006 and beyond, this slowing of mail flow being attributable to outmoded or legacy technology. Some of these providers have recently acknowledged their performance problems to their customers.

The two key reasons Managed Service Providers sight for their message delivery delays are:

1. The significant increases in spam and virus volumes.
2. Changes in the message formats and delivery strategies used by spammers.

While these issues are realities on the Internet they should not be used as a convenient excuse for the fundamental failure by the service provider to meet their most basic and important obligation - the timely delivery of legitimate email messages to and from clients.

The root causes of the performance problems are technical:

1. **No true multi-tenancy:** The infrastructures deployed by Managed Service Providers are assembled using various software products that were originally designed for single company use. This configuration, combined with a simple SMTP relay infrastructure, does not allow them to assign system resources and full application control to each customer independently. Attacks targeting some of their customers will affect the processing and delivery of messages for all other customers sharing the same system.

“ Providers have hung onto last generation content scoring methodologies for spam and virus fighting. ”

“ Others struggle to accept that emails transiting Managed Service Providers can randomly take between minutes and hours to arrive at the intended destination. ”

“ Mimecast does not apply the flawed content scoring mechanisms that have both served and plagued the anti-spam industry for the past few years. ”

“ Spam now accounts for 90 per cent of the 50 billion emails sent each day, the majority of which is imaged based. ”

2. **No processing priority for good mail:** Managed service providers have implemented security methodologies that are predominantly focused on blocking bad emails and are not capable of intelligently prioritizing the processing and delivery of legitimate email messages at the same time. During attacks legitimate emails must contend with illegitimate messages for system resources, with malicious messages often winning due to the sheer volume of traffic they generate.
3. **Inefficient resource intensive tests:** Providers have hung onto last generation content scoring methodologies for spam and virus fighting. These methodologies require the full receipt of the message before rule processing can occur. As a result they incur a significant processing overhead and performance penalty delaying all messages during an attack or general increases in traffic generated by phenomena like spam 2.0.

Delivery delays may be tolerable or even undetectable by some clients; however many others struggle to accept that emails transiting Managed Service Providers can randomly take between minutes and hours to arrive at the intended destination. Before these changes occurred business emails usually took only seconds to be delivered.

Threats are evolving as financial rewards for successful attackers grow:

In 2006 we saw a dramatic shift in the content and delivery strategies of spam and in particular image based stock promotion or "pump and dump" spam. These delivery attacks are successful against current generation email security systems from software companies and managed service providers as vendors and services fail to keep pace with the technological advances of the spamming community.

These attacks publicly demonstrated the power that criminal gangs and those with malicious intent have over the Internet. They demonstrated an ability to command vast armies of "zombie pc's" or botnets, often for sale or rent, each capable of sophisticated attack behavior. Most worryingly however, when the evolving attack methodologies were studied closely it demonstrated that these criminals have an ever advancing knowledge of the multitude of email security technologies and how to breach them.

In November 2006, The Times, a leading UK broadsheet, published the following information.

- Unsolicited messages have increased by up to 300% over the past four months.
- Up to one in twelve computers in British homes are compromised, 600,000 are infected each day, with an estimated 80% of residential broadband connections in the US being compromised by botnets.
- Pump and dump image based spam now accounts for almost a 5th of unsolicited email, up from less than 1% in 2004.
- Spam now accounts for 90 per cent of the 50 billion emails sent each day, the majority of which is imaged based.
- 80% of spam is controlled by 200 gangs involving 500-600 professional spammers. Ten spammers, based mainly in Eastern Europe are responsible for most of the unsolicited messages.

“ ARMed SMTP is Mimecast's next generation email security methodology. ”

“ ARMed SMTP extends the standard SMTP stack by introducing a set of proprietary real-time countermeasures integrated with advanced security technologies. ”

“ Mimecast uses an On Wire approach to protect system resources from processing unnecessary, illegitimate or malicious email messages. ”

- In relation to pump and dump stock spam, Oxford University found that; if a spammer invests \$10,000 in a penny stock heavily touted through spam he stands to make \$133,000 over a two day period.

The Solution - Mimecast ARMed SMTP:

ARMed SMTP is Mimecast's next generation email security methodology. It overcomes the security, reliability, cost and performance problems faced by both companies and managed service providers and delivers comprehensive, scalable email protection.

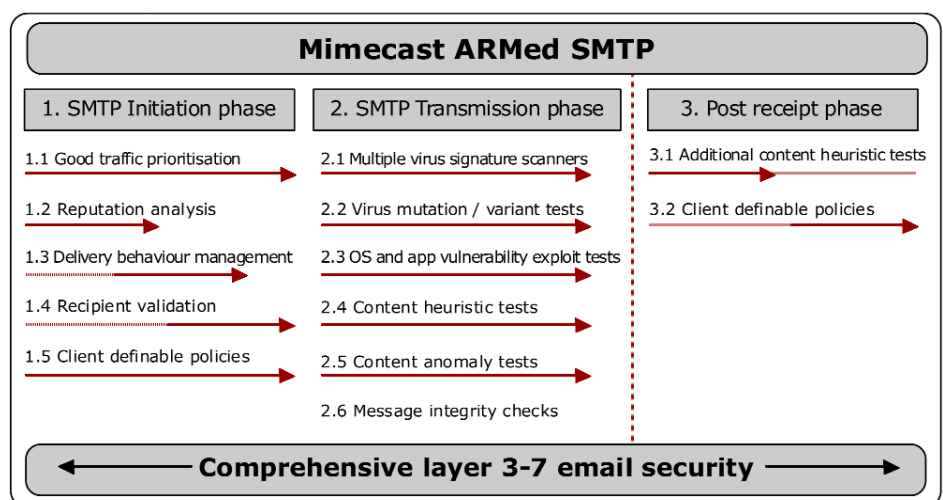
ARMed SMTP extends the standard SMTP stack by introducing a set of proprietary real-time countermeasures integrated with advanced security technologies to comprehensively address both known and unknown email threats at OSI layers 3 to 7.

How does it work?

ARMed SMTP applies security tests to email messages at every phase of the physical IP & SMTP conversation. To maintain the highest performance levels ARMed SMTP uses real-time protocol based techniques to look for the earliest possible opportunities to both reject problematic emails on the wire and to give legitimate messages processing priority. As the very first packets in a new SMTP conversation are sent *ARMed SMTP* works to assess the legitimacy of the message.

Legitimacy tests and risk assessments continue from the initiation phase of the SMTP conversation through to transmission & acceptance phase. Several tests are also applied post-receipt, as is end user policy control. *ARMed SMTP* incorporates a multitude of reputation tests, logic tests, pattern matches, anomaly tests and heuristic analyses most of which are applied in real-time to the byte stream.

The diagram below illustrates the 3 phases of delivery and several of the security tests applied by Mimecast.



How is this approach different?

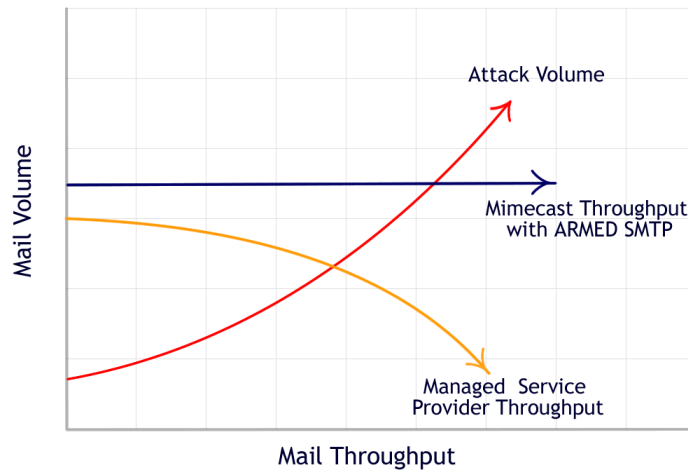
Mimecast's approach is sometimes referred to as an **on the wire** (On Wire) approach. It contrasts heavily with the traditional and dated **on the disk** (On Disk) approach used by most LAN based email security products and managed service providers.

“ Consistently 98% of attacks are thwarted at the SMTP initiation phase, 1.9% during SMTP transmission phase, and 0.1% of attacks are prevented post receipt. ”

“ Maintains a vast matrix of address to address white-lists and uses this information in real-time to avoid the risks of these unnecessary spam tests. ”

Traditional 'On Disk' techniques rely on the full receipt of the email message to perform the bulk of their security tests, whereas Mimecast's unique On Wire technology applies the bulk of the tests before and during the transmission of the bytes at the TCP/IP session. The On Disk approach is less effective as it consumes significant processing power and machine resources causing visible delivery slow downs at peak usage times and during virus and spam outbreaks.

On Disk methods are also heavily reliant on quarantines and quarantine management systems as once the message is accepted it often requires a human eye to determine if the classification has been correct.



Mimecast uses an On Wire approach to protect system resources from processing unnecessary, illegitimate or malicious email messages, without the need to write large amounts of email data to disk. This approach combined with Mimecast's unique Good Traffic Prioritization (GTP) technology make Mimecast the worlds only Internet based email security provider to offer holistic email security to overcome the various drawbacks of both LAN based and managed service provider approaches.

Additionally Mimecast is a fully integrated multi-tenant platform. This enables the ARMed SMTP protocol to intelligently customize its behaviour and assign resources to clients processing and delivery independently and in real-time without affecting mail flows.

| Traditional email security approaches | Mimecast ARMed SMTP |
|---|---|
| Can not distinguish legitimate traffic until after full message receipt if at all. | Intelligently prioritises legitimate traffic in real-time. |
| Performance degradation during spam /virus spikes and peak usage both inbound and outbound. | Maintains near zero-latency delivery performance levels during spam/virus spikes and peak usage. |
| Breaks the transactional integrity of SMTP via accept-then-reject/delete/quarantine processing. This risks losing messages and requires ongoing administration. | Maintains the transactional integrity of SMTP so messages are never lost and there is no administration overhead. |
| Effectiveness varies as illegitimate message content and delivery strategies are adapted to beat filters. | Consistently effective against all types of unwanted and malicious content. |

What results has Mimecast ARMed SMTP achieved?

1. Consistently 98% of attacks are thwarted at the SMTP initiation phase, 1.9% during SMTP transmission phase, and 0.1% of attacks are prevented post receipt.
2. Leaves 99.5% of spam undeliverable at source
3. 100% virus protection record
4. Zero content-based false positive email processing

To achieve these industry beating results, Mimecast began the development of an innovative next generation MTA early in 2003. Mimecast then significantly enhanced their SMTP stack to create ARMed SMTP. The above results have been consistently achieved since the system was introduced to market late in 2004. Today Mimecast is responsible for handling millions of messages for thousands of companies every day.

What is Mimecast ARMed SMTP particularly good at?

- blocking newly released (zero day) viruses before signatures are available by all commercial AV vendors
- blocking current, in the wild viruses and their variants
- preventing bespoke targeted email attacks from reaching your end users
- protecting your directory data from harvest attacks
- preventing email based denial of service attacks from reaching your network
- eliminating all types of spam - including image spam
- blocking phishing and scam emails
- maintaining optimal delivery performance of legitimate traffic during attacks
- preventing attacks made on one customer from affecting others
- avoiding the misclassification of legitimate emails as spam
- providing full visibility of your remote email ports
- enabling you to create exceptions and apply customized rules in real-time

The table below shows some of the layers or protection provided by ARMed SMTP and which work most effectively to counter various attack types.

| Types of Email Attack | Mimecast ARMed SMTP Layers | | | | | | |
|--------------------------|----------------------------|-------------------------------|----------------------------------|---|---|---------------------------------|--------------------------------------|
| | Reputation analysis | Delivery behaviour management | Recipient Validation via AD Sync | Signature and signature mutation analysis | OS and application vulnerability exploit assessment | Message integrity interrogation | Attachment heuristic risk assessment |
| Directed Attack | | | | | ✓ | ✓ | ✓ |
| Sabotage Attack | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Denial of Service Attack | ✓ | ✓ | ✓ | | | | |
| Directory Harvest Attack | ✓ | ✓ | ✓ | | | | |
| Scam Attack | ✓ | | ✓ | ✓ | | | |
| Spam Attack | ✓ | ✓ | ✓ | | | ✓ | |

One final critical success factor: Avoiding false positives

Mimecast works to repel both spam and viruses using ARMed SMTP. In practice, every time an anti spam provider tests a legitimate email they impose a level of delivery risk onto that message. Getting it wrong means that risk can translate into expensive losses for the company which was relying on the safe passage of that message.

Mimecast works in two ways to ensure that the risks of false positives are avoided:

Mimecast tracks outbound communications to learn and maintains a vast matrix of address to address white-lists and uses this information in real-time to avoid the risks of these unnecessary spam tests.

Secondly, Mimecast does not apply the flawed content scoring mechanisms that have both served and plagued the anti-spam industry for the past few years. Whilst in the beginning techniques such as Bayesian scoring worked to block spam successfully, spammers have now comprehensively tricked these systems into making entirely arbitrary decisions. Companies working with industries such as financial services and pharmaceutical suffer the most, but practically every user of email has experienced a legitimate email being misclassified as spam by a content scoring system.

Avoiding false positives, reducing administrative overhead, and guaranteeing the delivery of legitimate email has always been a key research priority for Mimecast. This has ensured that Mimecast users avoid the cost, risk and embarrassment of lost messages without the need to apply administratively intense quarantine monitoring.

Mimecast is different in seven important areas:

1. **Scope:** Mimecast is a 100% unified solution providing a single browser based command centre to manage all the traditionally disparate email management services like security, long term storage, advanced MTA functions, and email continuity.
2. **Control:** Mimecast is truly a multi-tenant platform which provides each customer with real-time visibility, constant control and instant configurability which removes all of the feature and control trade-offs usually associated with a managed service.
3. **Timing:** Mimecast can be provisioned and deployed for your business immediately so that your email management projects can meet deadlines or run ahead of schedule.
4. **Cost:** Mimecast costs at least 60% less than alternative approaches to email management enabling clients to get more and resolve all of the major email issues well within budget.
5. **Security:** Mimecast includes ARMed SMTP the industry's most robust and intelligent email security solution.
6. **Storage:** Mimecast's unique storage grid technology, Stor4, is fully integrated into the Mimecast platform offering the industry's most cost effective high performance long term storage, search, compliance and information management solution.
7. **Continuity:** Mimecast includes Always on Email, so that during any local disaster your end users have Mimecast as an alternative mail server with web based access to both new emails that can not yet be delivered to your server and historical mails. This makes a geographically resilient messaging infrastructure available to companies of all sizes.

About Mimecast

Mimecast is the leading innovator in the Software as a Service business email management market. The company provides best practice messaging security, storage, continuity, business information management and policy control to clients around the world via a unified internet based architecture. Mimecast was founded in late 2002, and is headquartered in the UK.

Where to now?

Mimecast offers a personal live demonstration via the web. To request a demonstration contact us on:

www.mimecast.com

info@mimecast.com