



MessageLabs Protect

"Spam will continue to be a significant problem for the foreseeable future, and organizations must aggressively erect a continuously adapting set of barriers to keep spam at bay. Anti-spam solutions that use a layered approach and multiple proactive and reactive detection techniques provide significant benefits over other models. They are highly accurate in detecting and blocking spam and effective at limiting critical false positives and are well-suited to defend against the ever-changing nature of spam."

**Matt Cain, Vice President,
Gartner Group**

An overview

Email has become one of the most important channels of communication for businesses, electronically linking them with their employees, partners, vendors, and customers. Consequently, keeping email secure and functioning has become a high priority. Every day, enterprises face potential communications, operations, and intellectual property disruption from spam, viruses, and other email threats. And every day, these threats become more malicious and sophisticated, creating security vulnerabilities, taxing infrastructures and escalating costs.

Viruses, spam, and harmful or unwanted content can seriously damage an organization. Spam and virus ratios rose over the past 12 months, during which time the virus infection average ratio was 1 in 16, compared to 2003 when it was 1 in 33. The most widespread virus outbreak of 2004 was MyDoom.A, which hit in January. Over the past few years, viruses have evolved to elude the limited advances made in the traditional anti-virus industry and have become even more destructive. Viruses have the potential to launch denial-of-service attacks and close down an organization for hours, even days. In addition, they can erase or steal critical business information, exposing a company to financial and operational risks as well as causing damage to its reputation.

The sophistication of email threats has evolved, going beyond just viruses and spam. The two distinct groups of virus and spam writers are now taking advantage of each other's methods. As a result, different types of email security attacks have started to merge and pose severe threats to your organization, leading to a significant increase in email related costs.

Uncovering the issues

Threats to information and infrastructure integrity

Information is the key business asset for all organizations. To secure this asset's integrity, organizations need to be able to measure their vulnerability to email attacks. They need to be sure that their security policy is comprehensive and that business continuity plans can mitigate the possible loss of data or business information.

Targeted attacks

Targeted email attacks come in a number of different guises, some more prevalent than others. Only the most sophisticated technology will keep threats such as malicious code, Trojan attacks, denial of service attacks, flooding, botnets and blackmail at bay – particularly with scriptwriters striving to develop new, more sophisticated techniques.

Indiscriminate attacks

Spam is easily the most prolific of indiscriminate attacks, impacting staff productivity as well as the capacity and efficiency of IT infrastructure and its associated costs. In January 2005, MessageLabs Intelligence reported that 83% of emails were identified as spam.

Spam is far more than a nuisance. Many studies have evaluated its impact on employee productivity. And businesses are now recognizing the need to manage and archive email communications more effectively to comply with increasing regulation. The burgeoning volumes of spam email can have significant impacts on storage and archiving costs. More disturbing is the growing use of spam to propagate fraudulent content, and steal personal information.

Providing solutions

MessageLabs reduces risk to businesses by protecting and controlling business assets and reducing their vulnerability to email attacks. The MessageLabs Protect services (Anti-Spam and Anti-Virus) offers multi-layered protection against all email-based threats such as viruses, malware, spam and phishing scams. Operating at Internet level, MessageLabs Protect combines best-of-breed commercial scanners with industry-leading predictive technology from MessageLabs Skeptic™.

“MessageLabs, offering up the right remedy to companies looking for managed e-mail security services, takes a proactive approach to threat elimination. The MessageLabs solution is one of the easiest IT implementations a customer can do.”

CRN gives MessageLabs five out of five stars for technology

MessageLabs Protect services mitigate the risks associated with known and unknown messaging threats, ensuring the continuity of your business communications.

As part of a complete managed email security solution, MessageLabs Protect ensures email continuity for your organization, meaning 24/7 availability of your mission-critical email services. With MessageLabs, email continuity is delivered through embedded protection and recovery, automatic email spooling and even distribution of email traffic. If your mail server goes offline for any reason or experiences a surge in email volume, MessageLabs simply queues the incoming messages and then delivers them when your mail server is back online.

Benefiting your business

Protect the continuity of your business

Mitigate the risks associated with known and unknown email threats to your business, ensuring the continuity of your business.

Protect your business productivity

Minimize the impact of spam on your employees and maximize productivity and predictability of your email infrastructure, ensuring email remains the vital business tool that it is today.

Protect your employees and information

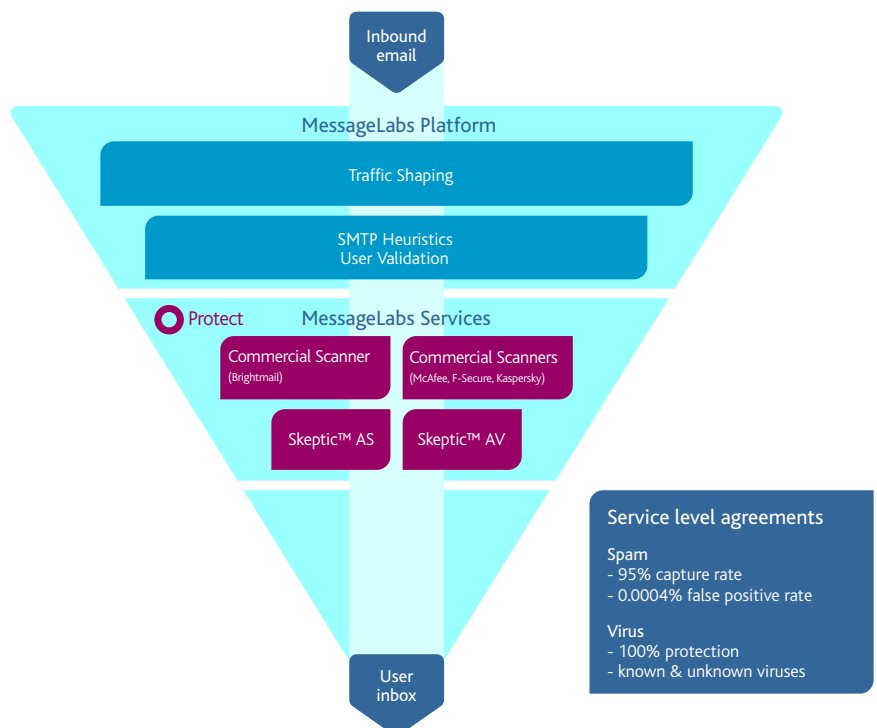
Safeguard your information assets from the risk of compromise through targeted email attacks, protecting your organization from loss of information via email-based identity theft.

Protect your corporate reputation and brand

Relax, knowing that your brand will not be compromised by malicious third-party campaigns.

Multi-layered approach

The most effective way to achieve long-term protection against viruses and spam is to implement a multi-layered defense system. The Protect services employ responsive and predictive layers of third-party and proprietary technology, ensuring that your corporate network is always protected.



Traffic management

As soon as email reaches the perimeter of the MessageLabs platform, at TCP/IP level, it is processed by our Traffic Management system. This acts as a router and analyzes packets in transit – before the email is received by the mail server.

It builds a knowledge base and profiles of all senders' IP addresses, allowing it to prioritize traffic. Known spammers are allocated fewer network resources and traffic is slowed – meaning that spam is suppressed, but never stopped, at this stage. Legitimate email traffic is sent by the quickest route to the next layer in the MessageLabs platform.

Connection management

Our proprietary SMTP Heuristics system works at the point of connection, with the aim of reducing the number of incoming connections. It is able to recognize and prevent brute force and denial-of-service attacks, keeping your network clear of malicious overloading.

Alongside the heuristic analysis layer, MessageLabs operates a User Validation process that compares incoming connections with a pre-populated list of valid mailboxes. If the destination mailbox is found to be invalid or non-existent, the email is rejected. Clients can upload and update their list of valid users via the Insight web interface.

Commercial scanners

In addition to Skeptic, multiple commercial scanners are used by MessageLabs to detect and stop all known threats. Commercial scanners offer a perfect compliment to Skeptic technology. While Skeptic has been designed to stop new and unknown threats, commercial scanners perform best at blocking previously seen malware.

Using database technology and pattern matching, commercial scanners compare potentially infected or inappropriate emails to all known signatures. If the signatures match, the particular email is identified and isolated. MessageLabs Protect uses Symantec Brightmail™, which incorporates the world's largest database of signatures.

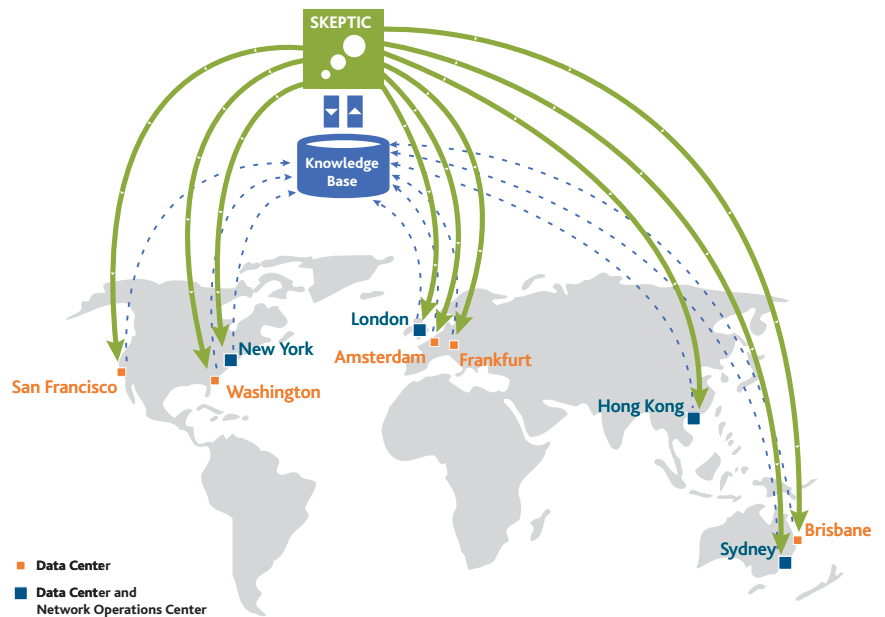
In order to stay up to date, commercial scanners update their signature files frequently – often several times a day during outbreaks. MessageLabs automatically receives all updates from the vendor and updates our engines immediately.

Skeptic™ Technology

Skeptic is our unique predictive technology and the result of over six years of development time. It proactively monitors, tracks and provides industry leading protection against emerging threats before they get near your network. Using predictive intelligence, Skeptic learns from every message it sees, updating and evolving with every new threat – constantly building on its already vast knowledge base.

Skeptic's position at Internet level means it scans millions of emails every day, always watching and waiting for any new threat. If it identifies techniques or characteristics indicative of a virus, spam, or other threatening content it tracks it, while alerting our support staff to investigate it further. Skeptic is actively monitored and is continually being enhanced by our experts.

Skeptic runs on the MessageLabs global platform, which is capable of far greater performance and functionality than is generally possible within client or server-based software. The global database replication architecture within Skeptic allows knowledge gained in one part of our network to be replicated globally in real time.



MessageLabs Anti-Virus

MessageLabs Anti-Virus service provides 100% protection from known and unknown viruses, trojans and other forms of malware, saving you countless hours and human resources otherwise spent dealing with outbreaks and the associated clean up. The service also helps maintain system availability and business continuity while improving overall network security. MessageLabs Anti-Virus uses multiple commercial scanners to identify existing threats and our own proprietary Skeptic technology to stop all unknown threats from reaching your network. The service is backed by a Service Level Agreement guaranteeing that no known or unknown email viruses or malware will reach your network.

MessageLabs Anti-Virus is simple to switch on, with minimum disruption. Once activated, all your inbound and outbound email is routed through the MessageLabs Service and scanned by Skeptic and multiple commercial scanners before being passed on to its final destination.

Updates are continuously and automatically performed across the network, with updates carried out in the event of a new outbreak, providing zero-hour protection from even the most advanced email viruses, worms and other forms of malware – before traditional AV signatures are available.

When a virus is detected, the email is automatically stopped and held in quarantine for 30 days. The sender and administrator receive immediate notification, allowing appropriate action to be taken.

"The prospect of having MessageLabs screening out viruses for us at Internet level, and updating signatures every ten minutes, was extremely attractive. Apart from the peace of mind it offered in terms of protection to our systems, it meant we didn't have to deploy someone in-house exclusively on updating signatures internally."

**Head of Systems,
Condé Nast Publications**

MessageLabs Anti-Spam

MessageLabs Anti-Spam dramatically reduces the amount of unsolicited messages reaching your business, eliminating the loss of productivity associated with reading and deleting spam and reducing related processing, storage and bandwidth costs. The service integrates Symantec Brightmail anti-spam technology and other best-of-breed technology and techniques alongside our own proprietary Skeptic technology to create a highly effective, accurate, and completely managed anti-spam solution. The service is backed by a Service Level Agreement that guarantees a spam capture rate of at least 95% and the assurance of a false positive commitment of 0.0004%.

To identify unknown and new spam, MessageLabs Anti-Spam uses Skeptic's predictive technology which incorporates thousands of heuristics rules, Bayesian learning, smart signatures, fuzzy fingerprinting and dynamic header analysis. Skeptic learns from each message it sees, evolving and updating in real time to actively protect against the latest spam techniques while providing near-perfect accuracy to virtually eliminate false positives.

Automatic rule updates are integrated into the global network and performed without any administration.

Symantec Brightmail Signature Technology

MessageLabs Anti-Spam service integrates Symantec Brightmail alongside its own proprietary Skeptic predictive anti-spam technology, creating a highly effective, accurate, and completely managed anti-spam solution.

Symantec Brightmail's anti-spam technology works to quickly identify all the latest known spam with almost zero possibility of false positives, while MessageLabs Skeptic's predictive technology focuses on stopping new and dynamic spam threats in the 'window of vulnerability' before a signature is available. This partnership gives clients the ability to combat spam with a truly multi-layered solution.

With this technology deployed into our global infrastructure, MessageLabs can leverage millions of Symantec Brightmail honeypots and spam traps for the latest catalogue of known spam signatures. Using only exact matches, this technique is extremely accurate and highly unlikely to misidentify a message as spam, meaning it has a negligible 'false positive' rate. Spam emails detected via this signature-based technology can be confidently blocked and deleted, eliminating a large body of known spam.

Symantec Brightmail is one of the leading anti-spam technologies on the market and has consistently been found to have superior effectiveness and low false positive rates. By integrating this software with its proprietary Skeptic predictive technology, MessageLabs has created a highly effective, multi-layered managed anti-spam service that enterprises of any size and industry can implement.

How it works

- The client points their Mail Exchange (MX) record to MessageLabs
- Email is directed through MessageLabs and handed to the client mail server
- Known spam is combated reactively using Symantec Brightmail, a commercial scanner incorporating the world's largest database of spam signatures. Known spam senders are also identified through client-configured blocked sender lists and available public block lists
- Known viruses are intercepted through signatures; unknown viruses are picked up by Skeptic
- Unknown and new spam is also proactively detected by Skeptic's predictive technology
- Email identified as spam is re-directed with multiple re-routing options, which include: block/delete; forward to bulk mailbox; appending of the message header; or quarantine
- When a virus is detected, the email is automatically stopped and held in quarantine for 30 days. Both the sender and the recipient are notified immediately
- Clean email is delivered to client
- All threats are managed away from the client network

Technical features of MessageLabs Protect

Below are some key features of the MessageLabs Protect services:

- Skeptic predictive technology is combined with multiple commercial scanners, including Symantec Brightmail, which incorporates the world's largest database of spam signatures
- Skeptic is designed to identify and combat new virus and spam threats in real time
- Multiple detection techniques offer protection from spam as well as from known and unknown malware, including email viruses, trojans and executable code
- Includes non-English (Asian) language filters
- The service is configurable to your needs: viruses and spam can be blocked instantly and quarantined, or else deleted, forwarded to a bulk mailbox or their header/subject appended
- Blocked or approved sender lists are fully customizable
- Transparent signature and knowledge-base updates are included
- 100% virus protection Service Level Agreement as standard, along with exceptional anti-spam guarantees
- MessageLabs Protect complements MessageLabs Control and Secure services

"On the spam front, 86% of the 90,000 incoming e-mail messages Arnold employees receive each day are stopped as spam by MessageLabs. With MessageLabs, we're not pressing the delete key 70,000 times a day. They're managing the cleanup for us. If the service saves each employee 30 minutes per month, that makes it cheap, any way you measure it."

VP of IT, Arnold Worldwide

Service level agreements

MessageLabs backs our Protect service with a unique Service Level Agreement for detection of both known and unknown spam and viruses. No one else offers such a guarantee.

- **Anti-Virus protection** – we promise 100% protection from email viruses. Credit is offered if a client's systems are infected by a virus which was not detected by MessageLabs
- **Anti-Spam protection** – we are committed to a spam capture rate of 95% and false positive rate of 0.0004%, or 1 in 250,000 emails (supported by data from the VeriTest Anti-Spam Benchmark Service Report). Credit is offered if MessageLabs does not meet this commitment
- **Service availability** – we promise 100% service uptime. Credit is offered if service availability falls below 100%. The client may terminate the agreement if service availability falls below 95%
- **Email latency** – latency is the average roundtrip time of email sent every five minutes to and from every tower. Credit is offered if latency exceeds two minutes
- **Fault response** – MessageLabs will respond immediately to Critical and Major issues affecting client email (times vary by client and issue type)

About MessageLabs

MessageLabs is the world's leading provider of messaging security and management services with more than 12,000 clients in more than 70 countries around the world. Delivered at the Internet level, across a global network of data centers, MessageLabs managed service scans a billion business emails each week, protecting companies from email threats, securing confidential information and enforcing email policies. MessageLabs services enable businesses to ensure the integrity of electronic communications and regulatory compliance, help manage and reduce risk, secure critical infrastructure and maintain the confidentiality of information.

For more information on the global leader on messaging security and management, please visit www.messagelabs.com

**www.messagelabs.com
info@messagelabs.com**