



Effectively Securing Small Businesses from Online Threats:

*Minimizing the Risks Associated
with Email, Web, and Instant
Message Communications*

“However, to adequately protect themselves and their stakeholders, SMBs must do more than merely establish internal communication policies; they must also use effective administration tools to manage existing policies, block unauthorized content and malware, and proactively monitor all communication-related behaviors on both an individual and group level.”

Source:
MessageLabs Intelligence
April, 2007

Executive Summary

Situation – Online Threats Have a Significant Impact on Small & Medium Businesses (SMBs)

While the Internet has proven to be a vital communications medium, it also presents a wide range of threats that can cripple a business. This is especially true for smaller organizations that lack the extensive enterprise-class IT resources necessary to defend against Internet threats. Small to medium-sized businesses (SMBs) receive as much and sometimes even more spam as larger enterprises but are less likely to thwart the dangerous consequences. This can have severe repercussions for SMBs from a legal, technical and company reputation perspective. In particular, external online attacks and internal misuse of sensitive information can impose significant brand and/or image damage to an SMB. This kind of publicity can cost an SMB the loss of essential business opportunities and long-term reputation damage.

Problem – SMBs Lack the Internal Resources to Effectively Address Online Threats

For SMBs, threats such as spam can very quickly become a silent killer, overwhelming the resources of a mail system or network before effective countermeasures can be applied. Unfortunately, smaller companies often don't have the time or specialized IT resources to install, configure, and maintain an appropriate array of security hardware and software to continuously address the scope of threats from the Internet. However, to adequately protect themselves and their stakeholders, SMBs must do more than merely establish internal communication policies; they must also use effective administration tools to manage existing policies, block unauthorized content and malware, and proactively monitor all communication-related behaviors on both an individual and group level. Also, they must be able to accomplish this level of security protection at a reasonable cost that does not impose a heavy financial burden on the organization to the point of negatively impacting bottom-line profitability.

Solution – MessageLabs Provides SMBs with Complete Protection from All Online Threats

MessageLabs is the leading provider of security solutions across all forms of information communications for the SMB marketplace. As a managed service, **The MessageLabs Complete Security and Control suite of services** offers a comprehensive set of communication security solutions to protect businesses from all email and web-borne threats. The service requires no additional hardware or software on a customers' network, conveniently removing the need for on-site maintenance and layers of complexity having to be added to the information infrastructure. MessageLabs provides SMBs with enterprise-class service and support that allow management to focus on the needs of the business, without worrying about the details of managing communications security. MessageLabs also uses a simple, affordable, fixed monthly pricing plan, based on the total number of users, rather than use volume, which makes it much easier to budget for this expense.

Result – Online Threats are Intercepted Before They Can Impact the Business

MessageLabs leading role in the security services industry is the result of an extensive commitment to research, investigation, and proactive threat tracking of all communications-related online threats. This knowledge is used to develop the most secure communications security solutions for SMBs by learning about threats and averting them **before** they can impact the business. The system works by first identifying threats outside of the SMB network and filtering items such as viruses and unwanted content before they enter the network.

With a global presence spanning four continents, clients in more than 80 countries, and an infrastructure capable of processing hundreds of millions of electronic communications each day, MessageLabs provides small and medium sized businesses with complete security and integrity for all communications activities.

Introduction: A New World of Online Threats

The Internet has proven to be a vital communications medium for worldwide commerce, but as an open and unprotected global network it can also present a wide range of threats that can cripple any business organization.

Several years ago, most Internet threats were relatively benign examples of a young adolescent's technical expertise but over time they have evolved into increasingly sophisticated domestic and foreign attacks that are designed to capture financial, personal, or strategic business information. Threats now come in the form of deliberately malicious acts, and exploitive opportunities for hackers and/or organized crime. The impact is serious, and the landscape of victims is getting broader every day. In response, no organization can afford to have its networks remain unprotected.

Spammers do not distinguish among the sizes of organizations they target. SMBs receive as much and sometimes even more spam as larger enterprises, but are less likely to have the defense systems in place to thwart it. For small businesses, spam can very quickly become a silent killer, overwhelming the resources of a mail system or network before an effective countermeasure can be enforced. In fact, according to statistics compiled by MessageLabs Intelligence, approximately one out of every 1.33 email messages is spam, one in every 126 messages contains a virus or Trojan horse threat, and one in seven employees will handle some form of harmful web content¹.

Many of these threats can entail severe repercussions from a legal, technical and brand or company image perspective. For example, the legal impact of an employee sharing internal company secrets with a competitor or downloading illegal or inappropriate images can incur expensive legal challenges for the business. These types of illegal actions can also cause significant damage in the form of negative publicity which can cost SMBs present and future business opportunities.

The magnitude of Internet threats and their consequences would make the prospect of protecting, managing and securing business networks and information a challenge for any organization. The fact is that smaller companies simply don't have the time or specialized IT resources to install, configure, and maintain an appropriate array of security hardware and software to continuously address the scope of online threats.

In order to ensure a more secure working environment, SMBs must not only establish internal communication policies, they must also use effective administration tools to modify existing policies, block unauthorized content and malware, and proactively monitor all communication-related behaviors on both an individual and group level. While a host of network appliances and software solutions may claim to address these security issues, they cannot offer the same level of expertise, ease of use, convenience, and control that an outsourced managed service provides.

MessageLabs Complete Security and Control suite of services is an innovative, service-based architecture that facilitates the administration and deployment of a complete email and web security suite providing protection for SMBs at a very predictable and manageable cost. This powerful solution for solving communication security problems leverages a highly-effective outsourced managed service approach.

This white paper will examine the many threats, challenges, and risks that SMBs experience as part of today's dangerous online environment. It will also present the advantages of MessageLabs Complete Security and Control suite of services, and how it compares with existing security solutions. Using MessageLabs, SMBs can be fully protected without expending an amount of time and resources that could negatively impact both business productivity and profitability.

Several years ago, most Internet threats were relatively benign, but over time they have evolved into increasingly sophisticated attacks that are designed to capture financial, personal, or strategic business information.



¹ MessageLabs Intelligence Report, "Small Businesses in the Line of Fire", April 2, 2007

The volume of online threats is growing faster than the number of messages being sent on the Internet.

Understanding the Communication Risks to an SMB

Online Communication threats come in many forms, including:

- **Email Spam** - unsolicited or undesired bulk electronic messages or emails that contain advertisements.
- **Viruses** - computer programs that can infect a computer or network without the permission or knowledge of the user when an email attachment is opened. Viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer.
- **Trojan Horses** - a program that, unlike a virus, contains or installs a malicious program (sometimes called the payload or 'keylogger') that records user keystrokes and the websites that are visited.
- **Worms** - a self-replicating computer program that uses a network to send copies of itself to other computers without any user intervention. Unlike a virus, it does not need to attach itself to an existing program.
- **Phishing Attacks** - (also know as Obfuscating URLs) - are criminal activities that attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out using email and often directs users to a bogus website in an attempt to obtain sensitive information
- **Spyware** - computer software that collects personal information about users without their informed consent.
- **Adware** - software with advertising functions integrated or bundled into a program by which information about the user's activity is tracked, reported, and often re-sold, often without the knowledge or consent of the user.

The volume of online threats is growing faster than the number of messages being sent on the Internet. According to a recent report from industry analyst IDC, between 1998 and 2006 the number of emails that were sent grew **three times faster** than the number of people emailing them in part because of the growth of spam². This is represented below in Figure 1.

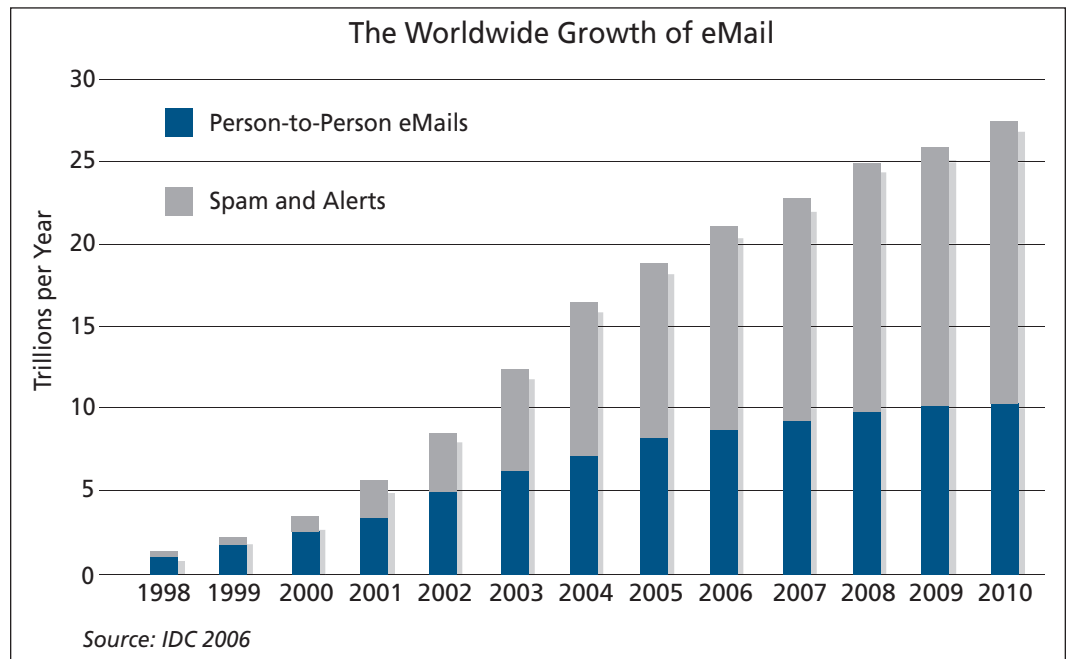


Figure 1: Spam Growing Faster Than the Number of eMails Sent

Given the scope of these threats and the damage that they can cause, SMBs must now become proactive instead of simply reactive in order to prevent attacks from inflicting damage.

² Source: IDC White Paper, "The Expanding Digital Universe", March 2007

The business risks that result from these online threats fall into four distinct groups:

- **Continuity Risks** - Continuity risks affect an SMB by degrading the effectiveness of existing business systems and preventing the continuity of normal business functions. Continuity risks can either be externally or internally generated threats. As an external threat, a continuity risk can come in the form of a massive spam attack that causes a network server to go down for hours or days. If such threats prevent essential business systems such as a Customer Relationship Management (CRM) or lead generation tool from functioning, the result could be a clear productive and financial loss for the SMB. As an internal threat, a continuity risk can be represented by the personal time that an employee spends on unwanted or unsupervised web surfing. In both of these circumstances, the continuity of normal business functions is altered.

- **Content Risks** - Content risks represent a threat to an SMB as the result of either the absence of a security policy or the implementation of a loosely-defined internal policy. Content risks can come from inbound information, such as inappropriate images that are downloaded into a company server, or outbound communications, such as email messages that are being hosted on a company server and sent out to the public containing illegal, inappropriate, or classified information. Some examples of content risks include:

- *Child pornography* downloaded to a personal folder on a workstation or server.
- *A terrorist site* that is being covertly co-opted and hosted on a company server.
- *Insider financial information* that is sent to an outside contact via an email message from an employee.

- **Policy Risks** - Policy risks are threats that are the result of poor or ineffective communication security policies. Strong communication policies are designed to move an organization from a reactive to a proactive response when illegal or immoral material or activities are detected. These policies prevent subsequent lawsuits or negative publicity that can inflict financial or reputation-related damage to an organization. For example, a security policy should indicate when the Human Resources department must be contacted and for what type(s) of infringements, or when enforcement law agencies should be brought in. Online security policies are intended to prevent situations such as:

- *A racial intimidation lawsuit* filed against the company as the result of profane email messages sent by an employee.
- *A sexual harassment lawsuit* as the result of sexually-oriented online material found on an employee's workstation or company server.
- *The failure to notify law enforcement agencies* when it has been determined that terror-related material is being hosted on a company server.

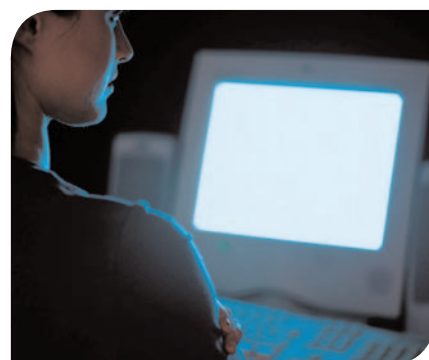
Online policies are not only designed to protect the SMB from illegal behaviors while employees are surfing the web, but they also provide administrative controls that prevent unauthorized viewing or access to certain websites or materials that could present a legal threat to the organization. Having these policies in place provides a framework to follow should legal action be required. These policies also extend to external business partners, clients, and vendors that have a working relationship with the company, and have access to the organization's network infrastructure.

- **Resource Allocation Risks** - These are risks related to a lack of resources which results in increased opportunities for external threats. Without a sufficient or well-trained administrative staff, or network hardware/software components able to spot potential threats and either prevent them or eradicate them, the SMB has an increased potential for a communication-related problem such as a virus, a massive spam attack, or the covert use of a workstation or server. Examples of resource allocation risks include:

- *Using outside consultants that are inexperienced* in addressing the latest communications security issues.
- *Network administrators who lack the proper training* to deploy appropriate solutions or spot trends that will either eradicate or prevent online threats.
- *Allocating an insufficient budget* for security tools and training.

Each of the four categories of risk outlined above increase the probability that inbound or outbound communications-related threats will be picked up by an Internet Service Provider (ISP), which can result in legal action by damaged parties or from a law enforcement agency such as the FBI. The consequences of such actions can include business interruption, monetary harm and corporate, brand and reputation damage which often has far-reaching, long-lasting and hard-to-repair effects.

A continuity risk can be a massive spam attack that causes a network server to go down or prevents essential business systems such as a Customer Relationship Management (CRM) or lead generation tool from functioning.



“Over 50% of U.S.-based SMBs that were recently surveyed showed that they had to act on some form of Internet abuse.”

Source:
Vanson Bourne on behalf
of MessageLabs
April, 2006

SMBs Are At a Greater Risk from Online Threats

The reasons for the lack of preparedness are no mystery. SMBs might feel they can't afford the **costs** associated with maintaining the internal hardware, software, and personnel resources necessary. Or, they can simply fail to take **proactive measures** to avert Internet threats. But, as a result of their lack of adequate protection, small to medium businesses are increasingly becoming the targets of spam, viruses, scammers, phishing attacks, and the hijacking of their network resources by online predators.

In fact, according to a 2006 survey conducted by Vanson Bourne on behalf of MessageLabs: of 942 IT decision makers, the 523 respondents from U.S.-based SMBs showed that over 50% indicated that they had to act on some form of Internet misuse. This burden usually falls on a human resources department or upper levels of management to resolve. The results of this survey are illustrated below in Figure 2.

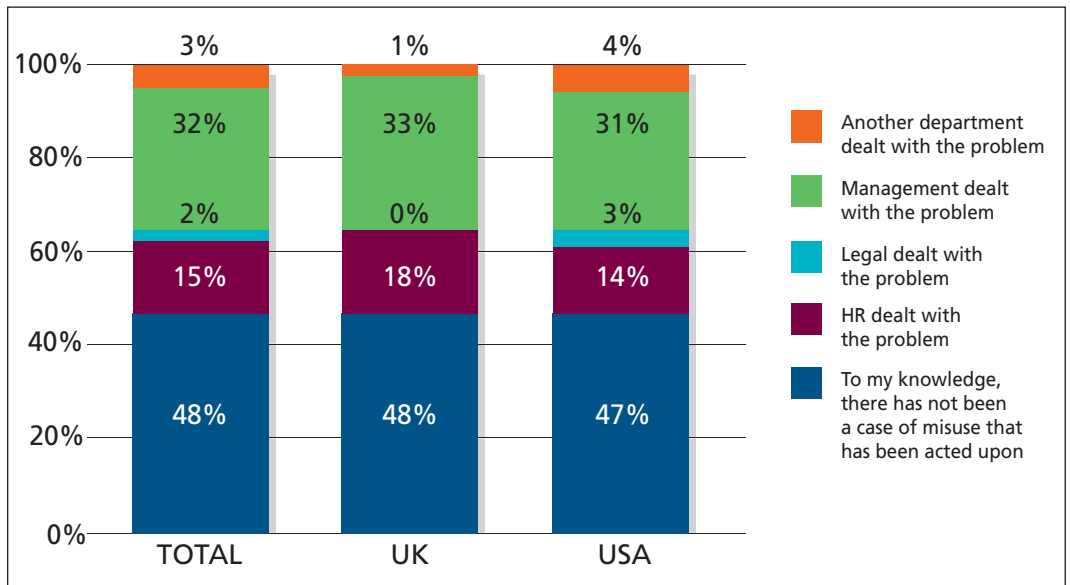


Figure 2: SMBs' Responses to Internet Abuse

Given the scope and potential impact of risks from the Internet, SMBs need to find an effective security strategy that allows them to take a proactive role in preventing internal and external threats. This requires an "enterprise-class" security protection strategy that has the robust capabilities of large business network security systems, but is affordable and manageable for a smaller business. The ideal approach would relieve the SMB from the burden of network administration and policy enforcement for all types of internal and external threats, and would offer an affordable pricing plan that accommodates SMB growth so the cost of maintaining ongoing security could be easily managed.

The Advantages of MessageLabs for the SMB

While appliance and software solutions were adequate as first or second-generation security solutions, the escalating and often unpredictable costs involved in supporting these “on-site” solutions — along with ever increasing scalability and performance issues — are leading more organizations to consider and adopt **managed services**.

Compared to on-site solutions, the managed services model offers a more complete set of solutions across a wider range of platforms. It works by identifying threats outside of the corporate network and filtering viruses and unwanted content *before* they enter the network. Additionally, managed services require no hardware or software on the client’s premises — thus removing the need for maintenance and layers of complexity added to the infrastructure.

The managed services model delivers a lower total cost of ownership and reduces the need for dedicated internal staff by providing a predictable cost structure and a limited need of internal resources for ongoing management and support.

There are three main areas where MessageLabs managed services approach delivers distinct advantages to SMBs for averting online risks:

1. Proactively stopping new trends and online threats
2. Offering a wide-range of security services
3. Access to a user-friendly online management portal
4. Providing a predictable total cost of ownership

1. MessageLabs Services Proactively Stops New Trends and Threats

MessageLabs leading role in the security services industry is the result of an extensive commitment to research, investigation, and proactive threat tracking of all communications-related online threats. This breadth and depth of knowledge and experience is used to develop the most secure communications security solutions available by uncovering threats and averting them **before** they can impact an organization’s information infrastructure.

Some of the investigative activities that MessageLabs conducts as an ongoing way of keeping their security solutions consistently aware of every conceivable online threat include:

- **Skeptic™ Technology** - Skeptic™ is MessageLabs proprietary security technology that proactively monitors, tracks, and provides industry-leading protection against emerging threats. Skeptic analyzes millions of email messages every day and uses the information it uncovers to update, evolve, and build a vast knowledge base of spam, viruses and online threats. If it identifies techniques or characteristics indicative of a virus, spam, phishing attack or other threatening content, it tracks the threat and alerts the MessageLabs support staff to investigate it further. This ensures that emerging threats are caught before they come anywhere near a client’s network.
- **Multi-Layered Approach** - MessageLabs pioneered the multi-layered technology approach using a “best-of-breed” third-party combination of technologies to identify known threats. This approach includes traffic management, connection management, and commercial scanners that work alongside MessageLabs Skeptic Technology to provide the most effective protection against online threats.
- **“Honeypots”** - A *honeypot* is a trap that has been set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. MessageLabs deploys honeypots across the globe to preemptively catch new online threats and modify security protocols to ensure that they never attack customers’ networks.
- **“Sandboxing”** - A *sandbox* consists of a tightly-controlled set of resources that are designed to safely run rogue or guest programs. MessageLabs uses sandboxes to analyze suspicious programs that have been downloaded from the Internet. The results from sandboxing techniques are used to update MessageLabs security applications and protocols.
- **“The WildList”** - The WildList Organization International is the world’s premier source of information on the viruses that are found on the Internet. When a threat is discovered, it is immediately sent to the WildList Organization so the threat can be made public. For the past five years, MessageLabs has been the leading contributor to the WildList as a result of the extensive investigative and pre-emptive activities that are conducted on a daily basis.

The managed services model delivers a lower total cost of ownership and reduces the need for dedicated internal staff, providing a predictable cost structure.



MessageLabs Complete Security and Control suite is the recommended choice for SMBs because it offers the most advanced protection in the industry against email and web-borne threats.

2. MessageLabs Provides a Wide Range of Security Services for SMBs

• MessageLabs Complete Security and Control Service

MessageLabs is the leading provider of security solutions across all forms of information communications for the SMB marketplace. Complete Security and Control suite is the recommended choice for SMBs because it offers the most advanced protection in the industry against email and web-borne threats. This suite also deploys 100% effective internet-level defense against spam, viruses, phishing, spyware and other malware conveyed via email or the web. In addition, it allows fully customizable control over all web traffic and email content entering and leaving your organization, protecting you from legal risks. The capabilities delivered by the Complete Security and Control suite provide SMBs the appropriate level of protection needed to effectively safeguard business communications, ensure business continuity, help control costs, and free IT staff to focus on business-enhancing initiatives.

An overview of the MessageLabs Complete Security and Control service suite is illustrated below in Figure 3.

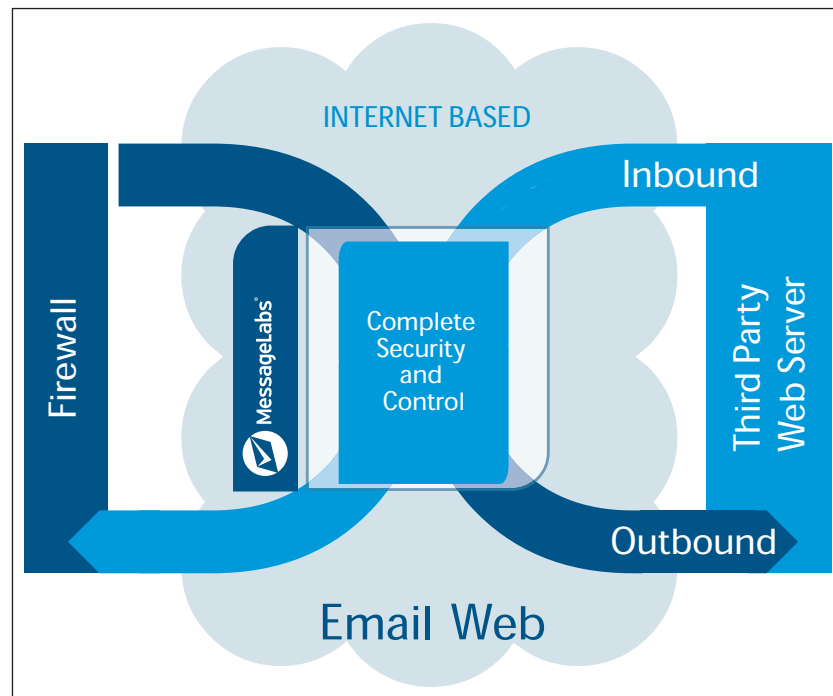


Figure 3: MessageLabs Complete Security and Control Service

• MessageLabs Archiving Service

Today, email has the same legal significance as paper-based information and managing it must be a top priority for businesses. The MessageLabs Archiving Service provides an industry-leading, cost-effective email storage and management solution. It not only ensures total privacy and data security but also enables immediate access and retrieval of emails — even after they have been archived. MessageLabs Archiving Service is also helpful in business situations where email records need to be stored for regulatory compliance and/or legal record verification purposes.

The MessageLabs Archiving Service frees IT administrative staff from the expense and effort needed to store huge amounts of email in-house, as well as the resulting network inefficiencies. MessageLabs managed service incorporates easy-to-use search and retrieval functions, supervision and reporting capabilities, and many other features necessary to satisfy both business and legal requirements.

• MessageLabs Enterprise Instant Messenger Service

Instant Messaging (IM) is an important part of today's business communication strategy. However, the use of public IM or mismanaged IM networks can lead to security threats to your organization. Key concerns associated with using uncontrolled public IM networks — such as Yahoo Messenger, AOL AIM, and MSN Messenger are increased viruses, trojans, malware, spam (spam over IM), identity theft, and exposure of confidential data.

The MessageLabs Enterprise Instant Messenger (EIM) Service allows employees to enjoy all of the benefits of a standard IM service without any of the associated risks. EIM provides a secure, private IM network that allows in-house employees, remote workers, and business partners to securely send and receive messages, save and search IM sessions, and simultaneously exchange messages and files. EIM File Sharing enables users to transfer files of any type or size, whether the recipient is online or not, reducing the burden on users email inboxes. In addition, it incorporates sophisticated administration, monitoring, and comprehensive message-logging capabilities. The service is not limited to EIM users; it enables users to collaborate with other popular messaging services such as Yahoo, MSN, or AOL.

3. User Friendly Online Portal - MessageLabs ClientNet™

MessageLabs ClientNet™ (Figure 4) is a user-friendly portal that manages all customer email and web services. It allows SMB IT and network administrators to run statistical reports on user online behaviors and viewed websites, as well as set or implement security policies throughout the organization.



Figure 4: The MessageLabs ClientNet™ Administration Tool

ClientNet features include:

- **Service configuration:** enables clients to set policies, customize actions for specific threats, manage quarantine settings and specify service notifications.
- **Service reporting:** provides a dashboard of valuable information for messaging environments, and detailed, customizable reports on each client's specific email and web threats, as well as individual recipients and policy compliance.
- **Online support:** includes a range of support options such as Knowledgebase Search, Support Ticketing Center, Service Guides and customized support contacts.
- **Service alerts and updates:** enables real-time alerts regarding the status of MessageLabs services and notifications of new service features.

The MessageLabs Enterprise Instant Messenger (EIM) Service allows employees to enjoy all of the benefits of a standard IM service without any of the associated risks.



MessageLabs pricing plan uses a simple, fixed monthly rate based on the number of users in the organization rather than the volume of communications use.

4. MessageLabs Services Provide SMBs with Predictable Costs

Many businesses employ the “appliance security model”, in which an increasing amount of hardware and/or software applications must be added to the network infrastructure as the number of users, capabilities, or volume of email/web traffic grows. These changing circumstances make the planning process for future needs difficult and add additional costs over time. This approach also adds heavy up-front costs from a capital expenditures perspective.

However, with a managed service such as MessageLabs Complete Security and Control Service, businesses are given **a predictable pricing structure** that helps better manage the cost of providing security. MessageLabs pricing plan uses a simple, fixed monthly rate that is based on the number of users in the company and the number of services that are requested, rather than the volume of communications use. This means that in the event of a large volume spam event, or a worldwide virus outbreak, the fixed monthly price does not change.

MessageLabs also provides SMBs with enterprise-class **service level guarantees** that allow the organization to focus on the needs of the business, without having to worry about the details involved with managing a communications infrastructure. As an outsourced service, MessageLabs allows each SMB to pick and choose the communication security services that best fit the needs of the business without the added cost of purchasing any additional hardware or software components.

The service also includes **24/7 service and support**, as well as access to end user tools such as an administration portal for managing security policies and spam quarantines. All MessageLabs clients benefit from a full range of service level agreements (SLAs), guaranteeing the complete certainty and continuity of business operations. MessageLabs industry-leading SLAs for service performance, service availability, and support response ensure the consistent protection for all customer business communications.

MessageLabs vast experience also translates into lower operating costs for their clients. The combination of SLAs and powerful self management tools are able to resolve technical queries without delay, around the clock. The MessageLabs team of client service managers, engineers and support personnel actively manage all email and web traffic every minute of every day. With their ability to analyze trends across the globe and stop threats before they can enter an SMB network, MessageLabs saves their clients from the costs associated with lost information, lost business opportunities, or the damage to the company brand or image that can result from online criminal incidents. With a global presence spanning four continents, clients in more than 80 countries and an infrastructure capable of processing hundreds of millions of electronic communications each day, MessageLabs provides small and medium-sized businesses with complete security and integrity for all their communication sessions.



Concluding Summary

It is a business certainty that the volume and ferocity of Internet threats are increasing at an exponential rate. Many of these threats pose risks that have the potential to cause catastrophic damage to an organization's reputation as well as to their private information, business data, or competitive standing. This can lead to a loss of productivity, loss of revenues, and sometimes even costly litigation.

It is difficult for a small to medium sized businesses (SMB) with limited internal resources to effectively battle Internet threats on an ongoing basis. To ensure the continuity and viability of the organization, SMBs must be able to address these threats before they can impact the business on either a financial, productivity, or legal level.

The **MessageLabs Complete Security and Control suite of services** provides SMBs with a complete portfolio of managed services that ensures the integrity of all electronic communications. This service allows an SMB to manage and reduce risks, secure critical infrastructures and effectively enforce sound communications policies at a reasonable and predictable cost.

MessageLabs is the world's leading provider of messaging security and management services. There are four key business advantages that SMBs realize in choosing MessageLabs for email and web security. They are:

- **Fully Managed Services** - MessageLabs provides a comprehensive solution that is easy to manage and easy to deploy.
- **Predictable Cost** - MessageLabs security solutions apply a simple flat-cost approach that is based on the number of users (which is predictable) rather than the volume of communications usage (which can vary widely).
- **Market Leadership** - No single organization knows more about nor makes a greater contribution to the area of threat detection and prevention than MessageLabs.
- **Complete Protection** - MessageLabs provides SMBs with complete protection and control, on both a legal and technical basis.

For more information about MessageLabs, the Complete Security and Control suite of services, or other MessageLabs communication security solutions, please visit our corporate website at www.messagelabs.com or call us at (646) 519-8100.

The MessageLabs Complete Security and Control suite of services provides SMBs with a complete portfolio of managed services that ensures the integrity of all electronic communications at a reasonable and predictable cost.



Americas
AMERICAS HEADQUARTERS

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
T +1 952 830 1000
F +1 952 831 8118

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong
T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 14
90 Arthur Street
North Sydney
NSW 2060
Australia
T +61 2 9409 4360
F +61 2 9955 5458

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
T +65 6232 2855
F +65 6232 2300

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
1 Great Portland Street
London, W1W 8PZ
United Kingdom
T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands
T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium
T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
FeringasträÙe 9
85774 Unterföhring
Munich
Germany
T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

www.messagelabs.com
info@messagelabs.com

© MessageLabs 2007