



## SECURITY SERVICES

# E-Mail Protection Services

### Savvis' E-Mail Protection Services (Powered by MessageLabs')

#### The Need for Comprehensive E-Mail Protection Solutions

In the past ten years, business communication via e-mail has grown in volume and popularity, and e-mail has become a mission-critical tool that is required to connect organizations' global offices and remote employees. With that in mind, it is extremely important to keep e-mail communication flowing quickly and efficiently through your organization. However, e-mail systems supporting organizations of all sizes face daily threats from computer viruses that can disable systems for hours (or even days), Spam e-mail that can flood systems with non-business-related messages, and the exchange of inappropriate content that can subject an organization to potential litigation and public embarrassment. Powered by our technology partner, MessageLabs, Savvis is able to offer a complete portfolio of e-mail protection services to address each of these issues.

#### Anti-Spam Services

##### Spam: A Costly Threat to Organizational Productivity

Spam — the electronic equivalent of conventional “junk mail”— has become a global epidemic, costing businesses around the world millions of dollars a year in lost productivity, increased storage costs and higher bandwidth costs. When organizations choose not to employ effective Anti-Spam solutions, employees spend countless hours per week reviewing non-business-related messages, deleting the messages from their “In-Boxes” and removing their addresses from Spam mailing lists. (And, such address-removal requests can actually result in employees receiving a higher volume of Spam e-mail in the future, as the Spammer comes to realize that the addresses are valid and active).

Utilizing its Threat Watch knowledge base of global e-mail traffic patterns, MessageLabs estimates that approximately 3 out of 4 e-mail messages carried Spam-related content to their recipients in November 2007. For the most up-to-date reports, please visit the following Internet link:

<http://www.messagelabs.com>

The Anti-Spam services leverage MessageLabs' extensive knowledge base of global e-mail traffic patterns, and its experience with the ever-changing techniques used by Spammers to circumvent Spam filters. By leveraging our combined experience in combating Spam-related e-mail, your organization could significantly reduce the number of unsolicited messages that are received, allowing you to maintain productivity and potentially reduce

#### Advantages

- **Anti-Spam Service:**  
Allows your organization to maintain productivity, while reducing potential e-mail-related storage and bandwidth costs.
- **Anti-Virus Service:**  
Prevents costly e-mail disruptions prompted by Viruses, Trojan Horses & Malware.
- **Content Control Service:**  
Permits e-mail to be filtered according to rules based on your organization's Acceptable Use Policy (AUP).
- **Image Filtering Service:**  
Detects pornographic images distributed by e-mail, reducing risk of harassment and workplace hostility claims.

both storage and bandwidth costs. A more detailed summary of the service appears in the section below.

### **A Comprehensive Anti-Spam Solution**

The Anti-Spam (AS) Service is a fully-managed service, which uses dynamic heuristics to identify and stop spam that is sent to users in your organization, before it can place stress on internal systems or waste valuable time. The AS Service effectively prevents unsolicited e-mail from entering your system, by scanning all incoming mail at the Internet level. It then frees up employee resources, alleviates bandwidth problems that relate to the receipt of Spam messages and significantly reduces demands made on your valuable storage space.

Your e-mail is subjected to rigorous scrutiny for unsolicited messages with little delay, resulting in a service that is essentially transparent to organizational end-users. For example, even though incoming messages are rigorously reviewed for Spam-related content, the latency relating to the service is minimal — no greater than 2 minutes.

### **At the Core of the Service: A Powerful Predictive Technology**

MessageLabs' predictive technology (referred to as Skeptic™) is at the core of the Anti-Spam solution. The term “predictive technology” is based on the manner in which Skeptic works. It not only identifies unknown and new Spam by utilizing resources such as heuristic rules, commercial scanners and dynamic analysis of message headers, it also “learns” from each message it reviews. The “learning” process allows the protection to evolve, and for the protection to be updated in real-time, so that the latest Spam techniques may be addressed promptly. And, even though the service is updated on an ongoing basis, the number of “false positives” identified by the service is minimal, so that end-users will continue to receive their important messages.

### **Customizing the AS Service**

A key benefit of the AS Service is your organization's ability to manage and customize the service, utilizing an AS Web management interface. This “always-on” facility provides a powerful tool for configuring your full portfolio of e-mail protection services (including Savvis' Anti-Virus and Image Filtering services, which are addressed in upcoming sections of the overview). You're free to change your private white-lists and black-lists, by selecting IP addresses, domain names and specified e-mail addresses, per your business requirements.

In addition to screening your e-mail, the AS Service can also scan for globally-known offenders — companies and individuals who have demonstrated characteristics that are representative of junk e-mailing. These offenders are registered on recognized public black-lists. With the AS Service, you can choose whether you require incoming mail to be checked against the black-lists, on a per-domain basis. And, you can also specify your organization's white-list of domains, IP addresses and e-mail addresses, from which you are willing to receive e-mails which otherwise may have been treated as Spam.

### **Convenient Management Interface**

In addition to providing you with the required tools to configure the AS Service, the Web-based customer management interface provides a wealth of management information. For instance, your organization is provided with real-time reports and online service statistics, enabling you to conveniently review how the service is performing. The customer management interface also enables you to identify trends in e-mail activity.

### **Anti-Virus Protection Services**

#### **E-Mail-Transmitted Viruses Pose Heightened Threats to Organizations**

Today's e-mail-borne viruses show some important similarities to the e-mail-borne viruses of the past, in that they can shut down an organization's e-mail infrastructure for hours, or even days. However, today's viruses also show some important differences, in that they now have the power to launch Distributed Denial of Service (DDoS) attacks, pilfer critical business data or even erase valuable business records. As we have witnessed in the past, major virus outbreaks within an organization are likely to receive press coverage, negatively affecting organizational reputation and brand equity.

MessageLabs' Threat Watch knowledge base of global e-mail traffic patterns also tracks virus-related e-mail activity. Toward that end, the company estimates that approximately 1 in 102 e-mail messages carried virus-related activity to their recipients in November 2007. (Although the percentage is not very high, the potential threat resulting from each e-mail virus is extremely significant). For the most up-to-date reports, please visit the following Internet link: <http://www.messagelabs.com>

With this Anti-Virus Protection Service (powered by MessageLabs), your organization gains protection against the growing threat of e-mail-borne viruses.

#### **A Fully-Managed Anti-Virus Protection Service**

The Anti-Virus (AV) Protection Service is a fully-managed service that can be activated with minimal changes to your e-mail configuration, and with no requirement to purchase additional hardware or software, on your end. Once the Anti-Virus Service is activated, all inbound and outbound e-mail is temporarily re-routed and scanned by multiple scanners, before it is passed on to its final destination.

If a virus is detected, the infected e-mail is automatically routed to a secure server, where it is held in quarantine for a pre-determined number of days (based on the user configuration that resides on the customer portal). In turn, your organization benefits from having the infected e-mail out of circulation (thus bypassing the potential risk of an employee accidentally clicking on the virus-laden attachment, while managing a busy mailbox). Overall, the service dramatically reduces your virus-related risk.

When the quarantine time period expires, the e-mail is destroyed. In addition, the sender and the e-mail administrator may elect to receive immediate notification when a virus is detected, allowing appropriate action to be taken. In rare instances in which a quarantined e-mail is shown to be releasable on the customer portal, your organization may elect to release it from the secure server and have the e-mail sent to the originally intended recipient(s). The e-mail will be released to the first address on the original recipient list

(if the address is a group e-mail name or an e-mail alias, the e-mail will be released to all addressees in the group, or the alias). The Anti-Virus Protection Service also has the capability to redirect the infected e-mail to an alternate address, within 8 normal working hours of the receipt of a “Release Authorization Form” from your organization. For your protection, e-mails containing a particularly infectious or damaging virus may not be releasable, in which your organization will receive appropriate notification through the customer portal. In the case of a major breakout of a new virus, an alert message will be posted on the customer portal.

As noted with the Anti-Spam Service, the Anti-Virus Protection Service has no discernible impact on e-mail delivery times. In addition, MessageLabs’ Skeptic™ technology evaluates incoming e-mails, to determine whether they exhibit characteristics similar to viruses, Trojan Horses or malware, thus updating the protection to combat newly-developing threats. These continual and automatic updates of virus signatures provide “zero-hour” protection, sometimes prior to traditional anti-virus signatures being updated.

## **Content Control Services**

### **Risks Related to Acceptable Use Policy (AUP) Violations**

E-mail is a powerful and convenient communications medium, but the instantaneous nature of e-mail transmission can place your organization at immediate risk. Therefore, it is important to control the content that is sent and received by your organization, particularly when it could be damaging to your employees and your organizational reputation. In an increasingly litigious world, it is essential that organizations protect themselves (and their employees) from internal and external e-mail content threats.

### **Maintaining an Effective AUP with Savvis’ Content Control Service**

Savvis’ Content Control Service enables your organization to configure a rule-based filtering strategy, in line with your Acceptable Use Policy for e-mail communication. Content Control allows your organization to build a collection of rules against which incoming and outgoing e-mail is filtered, in accordance with the terms and conditions of the service. A rule is an instruction set up by your organization, which is used to identify a particular format of message, attachment or content, and has prescribed to it a particular course of action that should be taken.

The Content Control Service enables your organization to identify and control confidential, malicious or inappropriate content that is contained in incoming and outgoing e-mail. Combining the latest technology with configurable usage rules, the service incorporates textual scanning, lexical analysis and attachment controls. By leveraging these resources, Savvis allows you to maintain control, while managing and enforcing your e-mail policies.

### **Detailed Content Control Reporting**

Through the Insight customer portal, your organization is able to review results generated by your Content Control rules, in the form of daily, weekly, monthly and annual summaries, organized by both rule and by user. Reports containing service activity logs can be generated on a weekly or monthly basis, and provided to your organization, upon request. For your convenience, sample “screen- shots” from the customer portal appear in the Appendix, at the end of the overview.

### **Supported Content Control Environments**

Content Control supports modern e-mail servers that can forward e-mail, utilizing common e-mail MX records.

### **Image Filtering Services**

#### **The Threat of Litigation & Harassment Claims**

The immediacy of business-related e-mail communication has also permitted the immediate exchange of e-mails containing pornographic, or other inappropriate, material. This is especially important when we consider that e-mails containing “jokes” (often accompanied by photographs) can travel widely across organizations, even though what is considered a “joke” to one employee may be considered “patently offensive” to another. This dissemination of offensive material can ultimately result in workplace-related claims, and has a serious impact on employee productivity. In addition, corporate reputation may be negatively affected, should such claims become public.

#### **Restricting Distribution of Inappropriate Images through Savvis’ Image Filtering Service**

Savvis’ Image Filtering (IF) Service utilizes neural network technology to accurately detect pornographic images. The key to the service is its proprietary, heuristic understanding of what an image is portraying. Unlike most anti-pornographic scanning systems, which employ color-matching technologies, IF identifies pornography by a process of elimination, through an understanding of what the people in any given image may be doing.

#### **Detailed Image Filtering Reporting**

Like the Anti-Spam Service, the Image-Filtering Service provides detailed reporting, and can report patterns of pornographic material detection, to alert staff of breaches to internal Acceptable Use Policies. Options are available for specifying the level of pornography detection sensitivity, from low, to medium, to high. Your organization may specify the action that should be taken upon the detection of a pornographic image. These options may be determined independently for inbound and outbound e-mail, and should be consistent with your applicable policies.

Action options for e-mail that is detected as pornographic include the following:

- Logging only (providing statistics viewable via the customer portal)
- Tagging of the suspect e-mail within its header (for inbound e-mail only)
- Copying the suspect e-mail to a pre-determined e-mail address
- Redirecting the suspect e-mail to a pre-determined e-mail address
- Deleting the suspect e-mail

## Comprehensive E-Mail Protection Solutions

Savvis and MessageLabs are proud to offer e-mail protection solutions that enable your organization to maintain productivity, lower e-mail-related costs, protect your organization from costly and protracted litigation & maintain corporate confidentiality.

The E-Mail Protection Services are part of a broader portfolio of Security Utility services, which offer our customers flexible and scalable managed security offerings that don't require hardware or software to be installed, and are managed in a centralized fashion by Savvis. Additional Security Utility offerings include in-network firewalling, DDoS and worm attack mitigation for Wide Area Networks (WANs), and virtualized security components, such as hosted firewalls and intrusion detection systems. For most Security Utility Services, reports are available in a convenient customer portal. For your review, "screen-shots" of sample e-mail reports appear in the Appendix at the end of the overview.

## About MessageLabs

MessageLabs is the world's leading provider of messaging security and management services, with more than 16,000 clients in more than 86 countries around the world. Delivered at the Internet level, across a global network of data centers, MessageLabs' managed service scans a billion business e-mails each week, protecting companies from e-mail threats, securing confidential information and enforcing e-mail policies.

MessageLabs' services enable businesses to ensure the integrity of electronic communications, help manage and reduce risk, secure critical infrastructure and maintain the confidentiality of information. **Please visit MessageLabs at: [www.messagelabs.com](http://www.messagelabs.com)**

## About Savvis

Savvis, Inc. (NASDAQ:SVVS) is an outsourcing provider of managed computing and network infrastructure for IT applications. By outsourcing to Savvis, enterprises can focus on their core business while Savvis ensures the quality of their IT infrastructure. Leading IT organizations around the world have selected Savvis to help them improve their service levels, reduce capital expense and deal with the rising costs of bandwidth, energy, real estate, staff and expertise. As a pioneer in utility computing, Savvis understands and harnesses the latest advances in technology like virtualization, cloud computing and support process automation.

## Appendix: ClientNet/Insight Customer Portal “Screen Shots”

Figure #1 represents the ClientNet/Insight Main Page. Service Alerts and Service Updates appear on this page. In addition, the page includes a convenient E-Mail Services Dashboard for the Anti-Virus, Anti-Spam, Content Control & Image Filtering services. The Top 5 Virus threats are also summarized here, for your preparation and convenience.

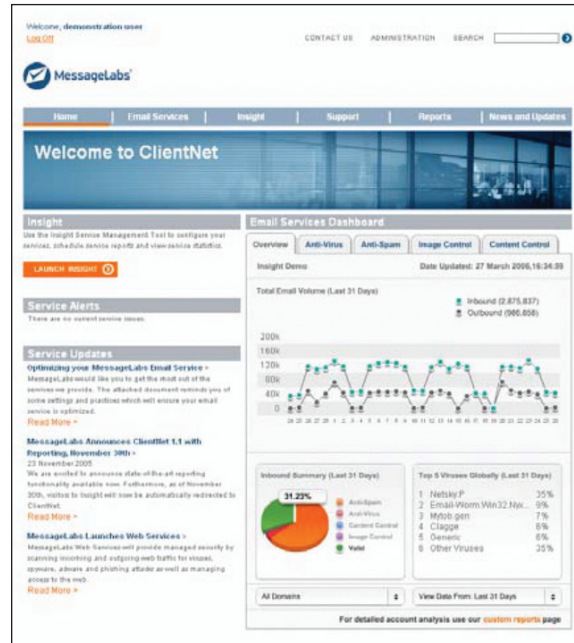


Figure 1

Figure #2 represents the ClientNet/Insight Reporting Page. As you can see, reports are available for the previous day, the previous 7 days, the previous 30 days, and for customer-selected date ranges. Domain ranges are chosen in the “Step 2: Select Domain” process that appears here.



Figure 2

Figure #3 represents the ClientNet/Insight E-Mail Services Page. This page summarizes your detection settings and quarantine settings for the e-mail protection services. In addition, maintenance may be performed on “approved sender” and “blocked sender” lists, at this location.

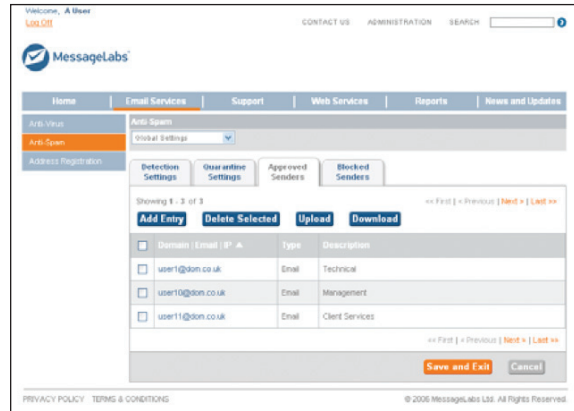


Figure 3

Figure #4 represents the ClientNet/Insight Technical Support Page, which contains a knowledge base of Frequently-Asked Questions from the MessageLabs user community.



Figure 4

**For more information  
about Savvis, visit  
www.savvis.net or  
call 1.800.SAVVIS.1  
(1.800.728.8471).**

EMEA  
Savvis UK Limited  
Tel +44 (0)118 322 6000

ASIA PACIFIC  
Savvis Singapore  
Company Pte Ltd  
Tel +65 6768 8000

JAPAN  
Savvis Communications K.K.  
Tel +81.3.5214.0151