MIMEsweeper™
policy-based content security

Advanced Content Security:

Protecting the integrity of your network and your business

January 2002

Table of Contents

Introduction

The Internet, for all of its world-changing benefits, presents businesses with a mixed bag of conflicting forces. It has certainly become essential for streamlining business processes and facilitating communication in today's connected economy. However, Internet connectivity also opens the door to an array of risks. Despite unprecedented investment in enterprise security, businesses continue to be hurt by network infiltrations, downtime and data loss due to computer viruses, confidentiality breaches and many other costly affects of the Internet.

As recently as five years ago, Internet security was widely considered synonymous with firewall deployment. Although firewalls are an important component of any organization's perimeter security, the continuing increase in network security breaches makes it clear that firewalls alone do not provide sufficient protection.

Security breaches, virus cleanups and other sources of downtime cause $1.39 trillion in lost business revenues worldwide in 2000.

Information Week's fourth Annual Global Information Security Survey

Similarly, virtually every Internet connected business uses anti virus products. These products are very effective at protecting organizations against known threats. However, despite virtually ubiquitous virus protection, 94 percent of respondents to the 2001 Computer Security Issues & Trends survey from the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) reported that they had been impacted by computer viruses in the past year. Anti-virus products surely play an important role in protecting networks from known viruses, but they have done little to deter the spread of new viruses and other malicious code, or "malware."

Other threats related to Internet use in the workplace have come to the fore more recently. Access to the World Wide Web has opened up an array of productivity-enhancing resources and applications for employees in all market sectors. Unfortunately, the Web has also proven to be an alluring distraction for employees, at best, and a mechanism for illegal and damaging employee activities at worst. Many organizations have installed URL blocking software that monitors and controls the use of the Web in the workplace. Again, while such solutions offer obvious benefits, they can only block known Web pages that have been categorized in their database, and they do not offer deep, customizable content analysis or protection from other Web-based threats.

This paper discusses how advanced, policy-based content security can be an enormously valuable addition to an organization's existing perimeter security and, furthermore, describes how to use this technology to enforce e-mail and Web usage policies that both protect the organization and enable additional business uses of the Internet.

What Is Advanced Content Security?

Content security refers to a broad spectrum of technologies designed to filter e-mail, Web and other Internet content. To maximize perimeter and internal network security, deploy advanced content security applications as a supplement to the firewall and related products such as anti-virus applications.

From a network security perspective, the firewall generally allows e-mail, HTTP or FTP content destined for Port 25 or Port 80 into the network. So how do we ensure that content allowed to pass the network perimeter is not a threat? Content security products include anti-virus software, malicious code filters and URL blockers. These products compare e-mail messages or Web content with frequently compiled databases of virus signatures and URL's to detect threats and take preventative action. Unfortunately, these content security applications are unable to combat new or well-hidden threats. That is, they are effective at detecting known threat "signatures," but are ineffective when the threat takes a new form.

Advanced content security extends well beyond protection from external threats originating from the Internet. Like antivirus and URL filters, these technologies analyze content as it enters or leaves the enterprise, allowing appropriate information to pass, and blocking — or taking some other protective action — to prevent transmission of restricted content. However, advanced content security products, such as the MIMEsweeper™ family of content security solutions, offer enterprise protection that is far more comprehensive in detecting content threats. Advanced content security provides three critical capabilities:

- **A policy-based structure** that integrates virus protection and other content security applications, maximizing the capabilities of each in a unified security framework.

- **Highly advanced content disassembly**, in order to filter and analyze the complete contents of an e-mail message or Web page for embedded threats that other scanners might miss.

- **Powerful text analysis, unparalleled format and encapsulation recognition and advanced threat disposal capability** that reinforce the security measures provided by the firewall and other applications.

Advanced content security builds upon the capabilities of individual content security applications to establish and enforce broad, flexible policies that protect the network while enabling effective and appropriate use of e-mail and Internet resources.

There is one final point regarding advanced content security. As you will see in the following sections, content-based threats are not just external threats. Advanced content security products, like the MIMEsweeper family of solutions, are designed to protect your organization from threats embedded in incoming e-mail and Web content as well as threats the move around and out of your internal network in the form of e-mail or Web content.

Content-based Threats

To fully understand how the implementation of advanced content security can benefit your organization, we must first define the meaning of a content security threat. We define threats in two categories: threats to an organization's network and threats to the overall integrity of the business.

Threats that directly target the computer network include e-mail-based or Web-based viruses and malicious code, unsolicited commercial e-mail, a.k.a. SPAM, and large message attachments that can degrade network performance

or even shut down network resources. Business integrity threats generally relate to the behavior of network users, and include loss of confidential business information, the circulation of inappropriate material, and copyright violations brought on by the use of unlicensed software. These activities may result in lawsuits, damage a company's market position and negatively affect its reputation with customers, partners and investors.

Content security threats exist outside as well as inside an organization, and are the result of intentional and unintentional actions. To better understand the potential impact of these threats, let us take a closer look at some specific threats and ways that advanced content security can detect and manage them.

Network Integrity Threats

Threats to enterprise systems continue to grow. Commonly we think of viruses and other malware as the primary threats to our networks. However, spam, large Internet file downloads or huge e-mail attachments can slow system performance or temporarily interrupt service. Network integrity threats also include theft and corruption of data, and degradation or loss of network services.

Viruses, scripts, macros and other malware

Although viruses are the most recognized form of content security threats, businesses continue to be vulnerable to new outbreaks. In the "2001 Information Security Industry Survey" by Information Security Magazine, viruses, worms, Trojan horses or other malware, despite the fact that 88 percent of those companies report having anti-virus protection in place, had infected 90 percent of the organizations surveyed. Clearly, organizations need to do more to improve their defenses against Internet malware.

Advanced content security offers several options for bolstering anti-virus security at the perimeter.

- **Integration with e-mail gateway, mail server and Web server anti-virus protection.** Among the most important features of an advanced content security solution is the ability to completely disassemble message content, including advanced formats, encoding and compression. Integrating your anti-virus and content security solutions will ensure that anti-virus scanners have complete access to all of the content of an e-mail message or Web download so they can stop otherwise hidden threats.

- **Text analysis.** Scanning e-mail and Web content for words, phrases and expressions commonly associated with malicious scripts or macros can enhance the protection provided by anti-virus software.

- **Detection of excess binary content.** In many cases, excess binary information can be an indicator of compiled malicious code embedded within seemingly harmless e-mail attachments and Web downloads.

- **Blocking high-risk files.** E-mail attachments and Web downloads can be denied based on specified file types.

Ninety-four percent of 2001 CSI/FBI survey respondent's detected computer viruses (only 85% detected them in 2000).

- **Handling encrypted files.** Policies can be configured to block or quarantine encrypted files from unknown or untrusted sources, as it may not be possible to scan encrypted content for malware threats.

- **Ad-hoc policies.** Security administrators can quickly take defensive action based on known information about a new malware outbreak. For example, during the I LOVE YOU virus outbreak, security administrators were quick to create ad-hoc policies that blocked any e-mail message containing the words "I Love You" until anti-virus pattern file updates became available.

Large file downloads and e-mail attachments

It has become common for employees to download the latest movie trailers from the Internet. This activity, by itself, may not represent a significant problem. However, when an employee attaches the movie trailer to an e-mail message and sends it to 20 or 30 friends and co-workers, serious network performance degradation could result. Of course, it is not just movie trailers causing the problem. Hefty presentations from the marketing department, or design documents from engineering also have the potential to bring a network down, if not managed carefully.

To effectively manage network resources using an advanced content security solution:

- **File-size restrictions.** Policies can be configured to limit the size of file downloads from the Web. Similarly, policies to block e-mail with specific types of attachments over a designated size (e.g., AVI files over 500 Kb) will reduce network congestion and may limit inappropriate Internet usage.

- **E-mail parking.** Parking large e-mail messages for delivery during hours when network activity is low is an easy way to protect network bandwidth. However, be sure to configure an alert for message recipients with instructions for contacting administration if the message contains urgent information that cannot be delayed.

- **Do not over-restrict.** Remember, some employees may have a legitimate business need to access or exchange large files via the Web or e-mail. Use the flexibility of your content security policy to enable legitimate and appropriate use of network and Internet resources.

Spam — unsolicited commercial e-mail

Junk e-mail sent to employee's cost one multinational corporation approximately one dollar per employee per day—a considerable sum given its 55,000 employees.

E-POLICY:
How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets

By Michael R. Overly

Unsolicited commercial e-mail, or spam, continues to be a growing problem for businesses. At the individual user level, spam is a nuisance and unwanted distraction. At the organizational level, the problem can be more severe. In a large organization, commercial e-mail campaigns may target many employees simultaneously, resulting in a flood of e-mail entering the organization. In severe cases, degradation of network service or even complete denial-of-service can result. Fortunately, using advanced, policy-based content security you can protect your organization from the threats associated with high-volume commercial e-mail.

Strategies for minimizing the impact of spam using advanced content security:

- **Limit the number of recipients** for an individual e-mail message.
- **Validate the message sender's domain** in DNS and validate the connecting hosts IP address using reverse-DNS lookup.
- **Use the Real-Time Black Hole List service** to identify and block known senders of spam.
- **Create your own lists** of banned e-mail addresses and hosts.
- **Create a content analysis policy** to search for common words, phrases and expressions used in spam messages.
- **Prevent the distribution of spam from your SMTP servers.** This is critical — you do not want your organization's domain name to be associated with the distribution of spam.

Business Integrity Threats

Network integrity threats can result in high recovery costs and cause a tremendous disruption to your business. However, it may be that threats to an organization's business integrity may have a greater impact, even though that impact may be more difficult to quantify.

What if a disgruntled employee sends your strategic business plan to your competitors? What if employees bring a lawsuit against your company because other employees are circulating pornographic material using e-mail? What if a mistake causes the release of e-mail messages containing private consumer information?

Each of these scenarios could cost an organization a lot of money. More important, in each of these scenarios, the most significant damage may be to your organization's reputation. Shareholders and benefactors may lose confidence in your ability to manage business affairs. Customers and partners may lose trust in your organization's ability to protect their confidential information and manage the productivity of your employees.

Loss of confidential information

According to a Secure Computing Magazine article in August 2001, "about 90 percent of any company's intellectual property capital – their inventions or concepts – can be found in a digital format. Of that, 45 percent of those corporate ideas are stored in an organization's e-mail system."

The trend toward the use of electronic information and information exchange has created parallel concerns for the security of confidential business information. Recently, legislation protecting the privacy of consumer information, like the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), has significantly increased the pressure on organizations to establish and enforce strong information confidentiality policies. Regardless of legislative mandates, the protection of

confidential information should be a top concern for any business. It is notable that loss of privacy/confidentiality ranked #1 on the list of IT security concerns in the "2001 Security Industry Survey" by Information Security Magazine.

A common first step to improving the protection of confidential information is to invest in stronger network access-control policies and mechanisms. Unfortunately, when electronic information is the concern, many organizations forget to establish and enforce e-mail policies for the transmission of confidential information. It is a simple scenario; an employee with access to confidential information sends that information in e-mail to an unauthorized recipient. Sometimes this type of security breach happens intentionally, but often it is the result of a simple mistake. Either way, the potential impact to the organization can be enormous.

Advanced, policy-based content security technology provides an unparalleled mechanism for enforcing confidential information access rules in e-mail communication. The content security policy also provides an extremely effective solution for managing message encryption of confidential information sent to authorized recipients.

Thirty-four respondents were able to quantify losses due to theft of proprietary information at $151,230,100, combined.

2001 CSI/FBI Computer Security Issues & Trends Survey

To create effective policies for protecting confidential business information in e-mail, consider these strategies:

- **What is confidential?** Determine the information your organization considers confidential and develop mechanisms to consistently identify this information in electronic documents. Confidential information could include personnel information, customer information, partner information, price lists, strategic documents, design documents, trade secrets, passwords or anything else your organization determines is critical to your business.

The loss of business information through e-mail, some of it accidental (due to the informal nature of e-mail and the Internet) is valued at over $24 billion each year.

Gartner

- **Who can send it?** Define who is authorized to transmit confidential information via e-mail. Remember, your policies may be different depending on the subject matter. For example, senior marketing managers may have a need to share strategic marketing plans via e-mail, while you would not expect sales representatives to be transmitting this information.

- **Who can receive it?** Define who is authorized to receive confidential information. This includes recipients within your organization as well as outside.

- **Use encryption.** Set your content security policies to prevent e-mail disclosure to unauthorized recipients and to encrypt messages sent to external authorized recipients. Establish policies to block unauthorized use of encryption.

- **Use disclaimers.** Add a legal disclaimer to all outbound e-mail messages that outlines your organization's policies regarding the use of e-mail content.

- **The back door — Web-based e-mail.** Do not forget about Web-based e-mail applications such as Hotmail® and Yahoo®! If left unprotected, Web-based e-mail use can provide a wide-open back door for confidential information leakage. Apply confidential information

security policies to Web posting to ensure comprehensive protection of your sensitive information.

- **Cookies and scripts.** Set policies to protect against confidential information theft using cookies or Web-based scripts.

The process of setting policies for e-mail that reflect your network access-control policies may be challenging. However, given the potential impact of a significant breach of confidentiality, whether intentional or unintentional, it is well worth the time and effort.

Use of computing resources for time-wasting activities

The statistics speak for themselves:

- According to International Data Corp., thirty to forty percent of Internet surfing in the workplace is not business-related.
- More than Sixty percent of all online purchases occur during business hours according to Nielsen NetRatings.
- Seventy percent of all Internet pornography traffic occurs during business hours according to statistics from SexTracker.
- Employee monitoring by the Internal Revenue Service and the U.S. Treasury Department revealed that nonwork-related activities accounted for an average of 51 percent of the time employees spent online.
- U.S. businesses lost an estimated $50 million in workplace productivity when approximately 13.5 million workers used workplace resources to download the Starr Report and view the video of President Clinton's deposition over the Internet.

Most organizations allow some personal use of computer and Internet resources by employees. However, as the statistics show, severe misuse and unreasonable employee distraction can result if organizations do not enforce reasonable rules for personal Internet usage. To enforce reasonable policies for personal use of Internet resources:

- **Categorize Web sites** that employees may use freely during work hours and those that require some level of restriction.
- **Combine the use of URL blocking and Web site content filtering** to restrict or manage access to Web sites. URL blocking technology is excellent for establishing rules about known sites on the Web. However, each day Web masters add volumes of content to the World Wide Web. To detect and block unauthorized Web content that the URL scanner does not block, use advanced key word, phrase and expression analysis.
- **Allow access during certain times of the day** for certain Web site categories. For example, organizations may allow access to major

online shopping or stock trading sites during lunch hours or before and after normal working hours.

- **Implement anti-spam policies**, which are not only important for protecting network resources, but also minimize the amount of distracting and unproductive e-mail that reaches employee in-boxes.

- **Consider diverse job needs.** Remember that different employees and groups within the company may require different policy considerations. For example, members of the finance group may require access to online financial information for the performance of their job, while access to the same sites by engineers may be indicative of personal online activities. IT security, human resources, legal counsel and department managers should work closely together to establish policies appropriate to the organization's business needs.

Use of computing resources for inappropriate or illegal communications

Of course, the cost of time-wasting activities is often far greater than just the cost of lost productivity. The stories are very familiar and all too common. Four employees sued Chevron for $2.2 million because of an offensive joke sent through e-mail. The New York Times fired two-dozen employees and disciplined many more for sending e-mail messages containing inappropriate images and offensive jokes. A police officer in Washington State was even videotaped surfing pornography over the wireless Internet connection in his patrol car.

Inappropriate use of network and Internet resources by employees costs organizations millions of dollars as a direct result of legal costs, lost productivity and bad public relations. Establishing and enforcing policies against this behavior is critical for an organization.

- **URL and text filtering for Web content.** As with time-wasting activities, combine the use of URL blocking and advanced content security key word, phrase and expression analysis to prevent access to inappropriate Web pages.

- **E-mail scanning.** Scan e-mail messages and attachments for words, phrases and images typically associated with inappropriate humor, flame mail and other categories that could result in employee harassment complaints.

- **File downloading policies.** Establish policies to prevent downloading copyright-protected material without authorization. Software copyright violations can cost $150,000 per incident and result in up to five years in prison. Of course, unauthorized use of software on a computer network can also result in serious network security and performance concerns.

- **Incoming and outgoing.** Remember, it is important to scan internal e-mail as well as e-mail entering and leaving the organization and HTTP and FTP content for inappropriate content. Most e-mail related harassment complaints are result from internal messages. Messages

containing inappropriate content that leave the company can result in negative publicity and embarrassment for the organization.

Planning your content security policies

Because every organization faces different business circumstances, challenges, workplace culture, network architecture, etc., it is impossible to recommend a "default" strategy and set of policies that everyone should espouse. However, some obvious common denominators exist, and we can offer some insight about how to approach an advanced content security plan.

It is important to recognize that the hard part of implementing your policies is often in the planning. Typically, an organization has two key objectives. First, the content security policy must serve as a primary defense against threats to information systems. Second, the content security policy must enable the effective use of e-mail and Internet resources by employees to minimize threats to the business.

Start with your defenses against external threats

The first step in implementing a comprehensive content security policy is to reinforce your perimeter security against external threats. These policies include:

- Virus and malware defenses for SMTP e-mail and Web browsing
- Policies governing large file transmission, receipt and downloading
- Policies to prevent floods of incoming spam and the use of your mail servers as relays for the clandestine spam distribution.

Typically, these policies apply equally to all employees in an organization. There may be some exceptions for policies against the transmission or download of certain file types administrators can easily address. For example, IT staff members and product support representatives may need to download and distribute executable files to perform their jobs. With the small number of employees involved, education on the proper handling and licensing of downloaded software is generally a supportable and effective security measure.

Enforce internal policies for e-mail and Web usage

Once you have established and implemented your external threat defense policies, you must turn your attention to the more complex policies that will enforce effective and appropriate use of e-mail and Internet resources by your employees. The policies included in this category are:

- Confidential information and privacy policies
- Workforce productivity policies

- Inappropriate or illegal activity policies

These policies will likely be more difficult to define than externally focused security policies. The reason for this is simple. Different employees and functional groups will need to use e-mail and Internet resources to perform their job in ways that may violate policies applied to other employees or resource groups.

For example, a product manager for a manufacturing organization may need to share extremely confidential designs for future products with customers whose future products will depend on this information. You would generally not expect a human resources employee to share such highly confidential information with an outside organization. For that matter, you would not expect a human resources employee to have access to this information at all. The challenge is to plan and implement policies that allow individual employees to do their jobs without compromising the organization's security or placing the integrity and reputation at risk.

Planning these policies effectively requires the work of a cross-functional team. We recommend that IT security managers coordinate with human resources, legal counsel, functional managers and executives to define and enforce policies that protect the organization without applying restrictions that impact the ability of employees to effectively complete work assignments or negatively impact the workplace culture.

Managing confidential delivery and record retention

There is one additional aspect of your policy for e-mail to consider. Up to this point, we have focused on stopping behavior and information exchanges that are potentially dangerous to the organization. Of course, most e-mail communication is safe and appropriate. Advanced content security enables the management of processes that allow organizations to manage e-mail communication as they would paper-based communication.

When an important, time-critical paper document is sent to a business partner, companies are careful to use a courier service that maintains confidentiality and provides a record of the package delivery. This paper trail makes it easy to maintain a file of the document for future reference.

Today, a growing percentage of our business communication exists only in e-mail. Nevertheless, most organizations have weak processes for ensuring confidential delivery and record keeping for e-mail communication. Advanced content security provides an excellent mechanism for managing these processes.

Policy-based e-mail encryption

E-mail encryption is complicated, but it ensures the intended recipient and no one else receives messages. Unfortunately, because of concerns about the cost and complexity of the e-mail encryption technology, most organizations have not implemented it widely. However, advanced content security provides an alternative approach to securing confidential e-mail and managing the use of encryption that is cost-effective and easy to implement, and that requires minimal effort to support.

Say an engineer from Company A needs to send confidential design information to a business partner. Using its content security solution, Company A enforces a policy that requires encryption of all e-mail messages from engineering to business partners as part of their procedure for protecting proprietary information. The engineer sends the e-mail message just like any other message. The content security server scans the message and then encrypts the message for delivery to the intended recipient.

This scenario could apply to a physician sending health information about a patient, financial institutions exchanging consumer credit information, or retail outlets forwarding customer lists to headquarters. The fundamental issues are the same. Organizations have many employees who share private, confidential or proprietary information using e-mail as part of their job. It is a good business practice, if not a legal requirement, to encrypt confidential e-mail to prevent interception of the message content by unauthorized recipients. By utilizing the content security policy to manage encryption, organizations benefit from comprehensive application of security policies and transparent encryption of confidential e-mail without end-user involvement. Furthermore, policy-based encryption management enables flexibility in the choice of encryption processes.

To exchange e-mail between large organizations, S/MIME gateways provide transparent, policy-based encryption using a single encryption key for each organization. For exchanging e-mail with small organizations that do not have established encryption capability, a variety of secure, Web-based technologies are an option. In cases where maximum security is required, special policies can enable the use of client-based encryption technology. Administrators can even apply content security policies e-mail messages and attachments after delivery, using advanced digital rights management (DRM).

For many organizations, it is conceivable that multiple encryption processes and technologies will be required to support a comprehensive confidential e-mail policy. Combining multiple encryption processes using client-based technologies would be unmanageable. However, automating multiple encryption policies as a function of the content security policy is relatively simple.

Policy-based e-mail archiving

Another important practice, and in some cases a legal requirement, for business e-mail is to employ retention and archiving policies. Again, the content security policy is an excellent tool for transparently enforcing this policy.

In general, it is not necessary to keep a record of all e-mail. Messages sent to arrange a lunch or dinner meeting probably would not be relevant for business records. However, organizations should retain messages that include sales proposals, nondisclosure agreements, contracts and other important business communications for some period.

The analysis capabilities of an advanced content security solution enable an organization to set policies that make an archive copy of important business communications. Administrators can easily create policies to support multiple categories. For example, an organization might want to maintain sales archives separate from human resources or finance archives. As with e-mail encryption, automating the archiving process through the content

security policy allows organizations to devise complex solutions that are easy and cost-effective to implement and manage.

Establish, Educate and Enforce

Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff, and empower those tasked with information security.

2001 CSI/FBI Computer Security Issues & Trends Survey

The fact that you have read this paper suggests that your organization is ready to establish and enforce a policy for the use of e-mail and Internet resources, if it has not done so already. Unfortunately, statistics show that many organizations forgo one of the most important steps in the process. In a recent American Management Association survey, 80 percent of employers indicated that they are establishing "e-policies." However, only a little over 50 percent of the employers surveyed indicated that they have employees read and sign those policies.

These survey results raise two concerns. First, organizations that do not proactively inform employees of rules and policies associated with e-mail and Internet use may end up defending themselves in harassment, wrongful termination or invasion of privacy lawsuits. Second, employees who do not know the policies will tend, through ignorance, to break the rules, resulting in a higher rate of security transgressions for the organization to deal with.

Enforcement — that is, implementation of an advanced content security solution — is really the third step in the process of policy development that we call the Three E's: establish, educate and enforce.

Organizations should work through the Three E's in order. First, establish a comprehensive policy for computer, network and Internet resource use and have every employee sign this policy. Second, initiate an ongoing education program to help employees understand the potential risks of e-mail and Internet usage. The best security that any organization can have is employees who make the right decisions. When these steps are complete, deploy MIMEsweeper solutions in concert with your firewall and anti-virus applications to secure your network, protect your business integrity and automate complex processes for managing business e-mail.

About MIMEsweeper

MIMEsweeper is the world's leading family of Web, email and Intranet content security solutions. More than 10,000 customers and 10 million users globally, use the award winning MIMEsweeper solutions to protect their networks and business from email and Web-based threats. The MIMEsweeper Family of products includes MAILsweeper for SMTP, MAILsweeper for Exchange, MAILsweeper for Domino and WEBsweeper. Combined these products provide organizations with an unparalleled content security solution.

Europe

United Kingdom
1310 Waterside,
Arlington Business Park
Theale
Reading
Berkshire, RG7 4SA

Tel: +44 118 903 8000
Fax: +44 118 903 9000
info@mimesweeper.com

Germany
Amsinckstrasse 67
Poseidonhaus
Hamburg, 20097
Germany

Tel: +49 402 399 90
Fax: +49 402 399 9100
info@mimesweeper.com

France
92 Avenue de Wagram
Paris, 75017
France

Tel: +33 172 74 6302
Fax: +33 172 74 6301
info@mimesweeper.com

America

USA
15500 SE 30th Place
Suite 200
Bellevue, WA 98007
United States

Tel: 425 460 6000
Fax: 425 460 6185
info@mimesweeper.com

Asia Pacific & Japan

AUSTRALIA
Level 4, Building C
CityWest Office Park
33 Saunders Street
Pyrmont
New South Wales 2009
Australia

Tel: 61 2 8514 7300
Fax: 61 2 8514 7301
info@mimesweeper.com

JAPAN
New Otani Garden Court
8F
4-1, Kioichi-cho
Chiyoda-ku
Tokyo-to, 102-0094
Japan

Tel: 81 3 5212 3772
Fax: 81 3 5212 3788
info@mimesweeper.com

www.mimesweeper.com