

MIMESweeper™ for SMTP 5.2

World's #1 email content security solution

Securing against all email threats, including spam and viruses

Digital attacks are not only on the increase, but are also evolving. Keeping ahead of the game protects your organization from the vulnerability that exists, before anti-virus and security companies issue patches and updates to deal with the urgent threats. Inefficient patch management enables virus writers to take advantage of these "Zero-Day" threats that can cost millions in damage to systems. In addition, inappropriate material, legislation, regulation and confidentiality are all areas of increasing concern and should never be underestimated.

IT managers are moving away from a piecemeal, point solution approach to content security towards embracing enterprise-class content security solutions. They want systems that deliver a lower cost of ownership and cost less in bandwidth and storage terms.

Clearswift understands that organizations of all sizes cannot afford to cut corners when securing mission-critical email applications. You need to be able to rely on best-of-breed solutions that provide total peace of mind. Since its original launch in 1995, MIMESweeper for SMTP has been widely regarded as the world's most powerful content security offering and the only solution worth considering.

MIMESweeper for SMTP

MIMESweeper for SMTP is the most sophisticated and versatile content security solution available today. It meets the needs of medium and large businesses alike, in markets as diverse as finance, banking, government, manufacturing, retail and high-tech.

Unlike other security solutions that provide protection against only one or two threats (i.e. specific anti-spam solutions, anti-virus solutions, anti-spyware solutions), MIMESweeper for SMTP addresses all the content security threats - before it's too late.

MIMESweeper for SMTP allows automatic updates to help defend against Zero-Day attacks. Automated ThreatLab™ alerts, including phrases, scripts and file checksums, update the software without manual intervention. This not only ensures protection against emerging threats, but also reduces the time and cost of keeping the security defense ahead of the game.

MIMESweeper for SMTP provides the following:

- **Policy-based Content Security**
 - Hierarchical roles-based security
 - Personal Message Manager
- **Advanced Threat Management**
 - Proactive automated update mechanisms
 - Layered anti-spam solution
 - Advanced anti-virus checking
- **Advanced Remote Administration and Reporting**
 - Secure policy management and administration
 - Single point for policy configuration across all servers
 - Consolidated quarantine management
 - Multiple Administrator accounts with concurrent access capabilities

Lowers TCO and tangible ROI

MIMESweeper delivers a lower cost of ownership and reduces the burden on the IT department through its innovative management interface. This framework integrates your SMTP gateways through one web-based management console, thereby simplifying administration tasks and ensuring policy enforcement across your organization. The automatic ThreatLab updates ensure that your system is always ahead of the game in combatting new threats, saving time and money on manual intervention.

Furthermore, your organization can significantly reduce bandwidth and storage costs created by large email volumes through the automatic compression of files.

The Issues:

Security: Viruses, Trojans and malicious code can all be transmitted via email. With the vast majority of business communications being carried out electronically, the chances of digital attacks are high.

Productivity: Loss of productivity is not just about employees' abuse of email and frivolous communication, often spam is the biggest culprit. Email users lose on average 10 minutes, and IT staff on average 43 minutes, each day dealing with spam.

(Source: IDC, 2004)

Legal liability: The circulation of offensive or inappropriate content, copyrighted material and corporate confidential information by email can lead to litigation and damaged reputations.

Compliance: Organizations face an increasing number of legislation and market regulations and are accountable for how information is stored, used and distributed. These regulations are not to be taken lightly as the repercussions could be crippling, through large fines and criminal and civil penalties.

Product Highlights:

- World's #1 content security solution
- Delivers Zero-Day protection through automatic threat updates
- Prevents virus infiltrations
- Blocks 98% of spam with zero false positives
- Proactive spam and threat updates keep systems current
- Highly scalable solution with support for up to 4 servers
- Handles 50 users as easily as 100,000 users
- Unique roles-based security allows enforcement of the most granular policies
- Easy-to-use policy wizards
- Intuitive web-based management interface
- Personal Message Manager allows users to manage their own quarantined emails
- Web-based Report Center with over 20 pre-configured reports
- Includes image analysis detection capability

The only solution to secure against ALL digital threats

MIMESweeper anti-virus protection - protecting against known and unknown threats

Clearswift surveys have shown that organizations fear virus infections above any other kind of digital attacks.

MIMESweeper for SMTP is designed to work with the AV tool of your choice. It intercepts and decomposes data flowing through the gateway, before passing it to the AV tools for virus checking and cleaning, providing ultimate protection against known viruses.

There is a significant vulnerability window that exists before anti-virus and security companies issue patches and updates to deal with urgent threats. However, MIMESweeper for SMTP is uniquely designed to intercept viruses, worms and Trojan horses unknown to AV vendors, thus protecting the integrity of your network.

The only solution to secure against ALL business threats

Loss of productivity

MIMESweeper for SMTP is designed to control and prevent abuse of email to ensure that systems resources are not eaten up by frivolous or unwanted messages. It features a comprehensive set of reporting tools that enables Systems Administrators to monitor daily usage, identify abuses, trends and map future requirements.

Compliance and legal liability

Organizations now face an increasing number of regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, SEC, Basel II, Data Protection Act, etc. They also have a duty of care to their employees, partners and customers. Exposure to objectionable or illegal content - be it pornographic, racist or just plain offensive - can cause costly litigation which businesses can ill afford. Loss of confidential information and intellectual property is yet another threat which can be disastrous for organizations and can ruin corporate reputation.

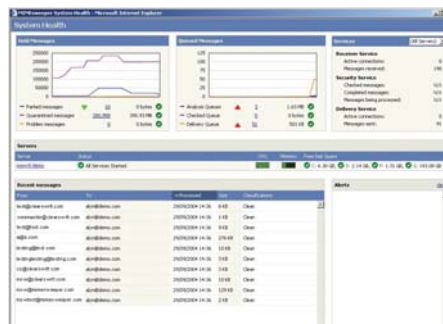
MIMESweeper for SMTP is uniquely positioned to address all legal liability issues and assist your organization to become compliant. Its powerful policy-based content security engine is designed to support policies as detailed or as simple as required. Its ability to scrutinize all the data passing through the SMTP gateway means that accidental or deliberate breaches of policy can be stopped before it is too late.

MIMESweeper anti-spam protection - comprehensive defenses adaptable to your environment

As the market leader in content filtering, fighting spam has always been an important part of our solution set. SpamLogic is the most accurate and easy-to-deploy solution on the market. It screens all email based on source, content and destination as well as all attachments and executables.

SpamLogic uses a whole battery of defenses, orchestrated in a completely new way to deliver the best accuracy rates you can get - up to 99%.

MIMESweeper for SMTP also provides validation of recipient addresses either using LDAP Address Lists or other manually entered data. As well as defending against spam emails, this validation prevents both anti-spoofing and directory harvesting.



Hierarchical roles-based content security

Content analysis is all about defining an employee usage policy that clearly states what an organization considers to be acceptable and unacceptable usage of the email and web systems. This policy must take into account the threats, legislation and regulation, in addition to the roles of individuals within your organization and their needs of the systems.

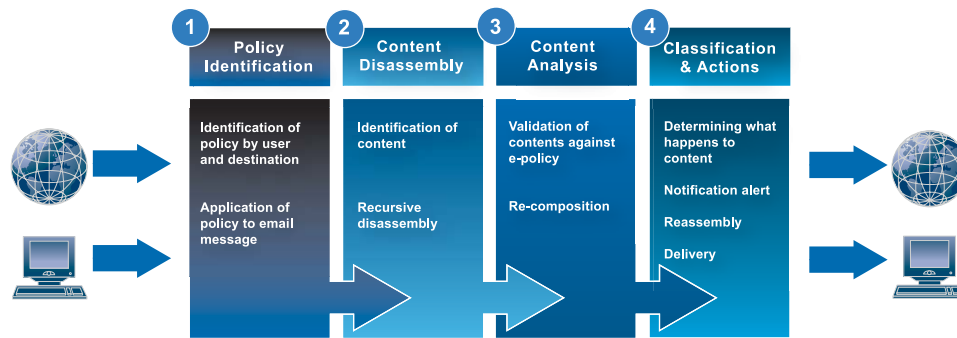
MIMESweeper for SMTP is designed to support corporate security policies and features a revolutionary roles-based security approach. Whereas most competing solutions can only turn functionality on or off, MIMESweeper for SMTP has embraced the concept of hierarchical security, and empowers your organization to apply varying types and levels of security for each user.

Exceptional scalability

Unlike competing solutions, MIMESweeper for SMTP is a long-term investment and a powerful backbone to email security. Designed to grow with your organization's needs, it can support companies with 50 users as easily as 100,000. By investing in MIMESweeper for SMTP, you can be sure that you've put your trust in a solution that will work now and into the future.

How does it work?

MIMESweeper for SMTP analyzes both inbound and outbound emails at the gateway in four stages:



Simplify your administration

Management and administration tasks on security systems can be a time consuming burden for IT staff. MIMESweeper's intuitive web-based management interface provides multiple Administrators with consolidated management all from one location, thereby saving time and effort. It includes five specific management areas:

- **Systems Center** - allows Administrators to control the services running on each host and view the status of messages
- **Security Center** - where Administrators' roles and responsibilities are defined
- **Message Center** - where the majority of the day-to-day tasks are performed. This Center provides a unified view of all the different quarantine areas and message directories thus simplifying the task of managing multiple servers, including detailed level message tracking.
- **Report Center** - where Administrators can access 20 pre-defined reports and a powerful wizard to customize reports
- **System Health** - a single web page that shows, at a glance, a snapshot of all the systems running in the configuration. It shows message flow, counts of messages in quarantines and passing through the system and key trend information (such as queue's getting bigger or smaller).

MIMESweeper's unique approach to system management allows for hierarchical devolvement of duties to multiple Administrators. IT managers can delegate specific responsibilities, such as server monitoring, access to particular quarantine areas and reporting, to the most appropriate Administrator or department; therefore spreading the load of administration and significantly reducing the time it takes to process blocked emails.

Message management

The growing volume of spam creates an enormous drain on IT department's time. According to IDC, IT staff waste on average 43 minutes per day simply dealing with spam. And this is merely checking whether blocked emails are spam, or releasing valid business emails which have been incorrectly categorized as spam.

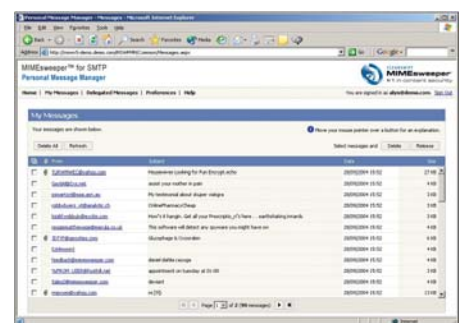
Personal Message Manager gives end users the power to determine whether their quarantined emails are unwanted spam. This key feature removes the burden of message management from the IT department and ensures that spam messages are more accurately identified.

In addition, the users can also configure PMM to display in one of eight languages - English, Japanese, French, German, Italian, Spanish, Chinese or Portugese - all on the same deployment.

Understanding your mail profile

For an IT security policy to be effective, knowing the way each organization uses email is as important as identifying the threats it faces. Report Center comes complete with pre-defined and comprehensive reports, viewable by secure connection from any standard web browser. The detailed and insightful graphical reports allow staff to:

- Demonstrate ROI using graphical reports
- Accurately analyze all email usage
- Audit and report on all email traffic, identifying peak periods
- Provide better capacity planning for improved efficiency and cost reduction
- Fine-tune policy to reflect the exact threats faced
- Understand the types of data contained within email messages



MIMESweeper™ for SMTP 5.2

Optional functionality

IMAGEmanager™

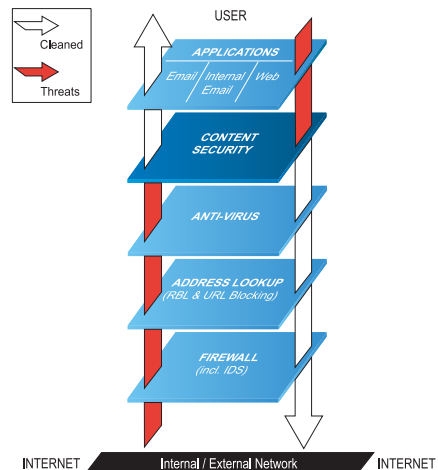
Using unique image analysis algorithms, MIMESweeper is able to identify and block pornographic or otherwise inappropriate images embedded within or attached to email messages. You can also add your own images to the database, ensuring that emails including confidential images, such as blueprint designs, can automatically be detected and blocked.

Total Content Security

As email and Internet usage continues to grow, the security policy is only as good as its weakest link. Mistakes or errors can cost businesses hugely. Most organizations do understand this and are starting to implement a layered security model consisting of multiple levels of additional and complementary security tools for all gateways and protocols.

Clearswift believes in multiple layers of defense at the SMTP gateway to ensure against digital attacks.

Complete Content Security - Content Analysis software works in conjunction with basic and entry level security systems to stop all unknown threats. In addition it scans content in real-time according to policy and permits or denies access depending on analysis of file type, text, images and embedded code.



Platform availability

Operating System

- Windows XP (SP1) / 2000 (SP4) / 2003 (English, French, German or Japanese)

Databases

- SQL 2000, MSDE, Oracle 9 for reporting

Directory Protocols

- MS Active Directory 200x / Exchange 5.5 and Domino directory servers

About Clearswift

Clearswift simplifies content security. Our products help organizations enforce best-practice email and web use, ensuring all traffic complies with internal policy and external regulations. Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic.

Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service. All three platforms are designed to take the hassle out of securing internet traffic, with a clear, intuitive management interface; automatic, 'zero-touch' updates; powerful reporting and common-sense policy management.

Twenty years of experience across 15,000 organizations has helped us raise security standards while simplifying security management at the same time. We've helped many of the world's most successful organizations use the internet with confidence and are committed to staying ahead of the market and helping our customers defend against all emerging threats.

Contact Clearswift

United States

100 Marine Parkway, Suite 550
 Redwood City, CA 94065
 Tel: +1 800 982 6109 | Fax: +1 888-888-6884

United Kingdom

1310 Waterside, Arlington Business Park, Theale,
 Reading, Berkshire, RG7 4SA
 Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Germany

Amsinckstrasse 67, 20097 Hamburg
 Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

Australia

Ground Floor, 165 Walker Street, North Sydney,
 New South Wales, 2060
 Tel: +61 2 9424 1200 | Fax: +61 2 9424 1201

Japan

Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku
 Tokyo 105-0011
 Tel: +81 (3) 5777 2248 | Fax: +81 (3) 5777 2249

MIMESweeper™ Email Managed Service

MIMESweeper™ SMTP Appliance

MIMESweeper™ for SMTP

MIMESweeper™ for Web

MIMESweeper™ for Exchange

MIMESweeper™ for Domino

e-Sweeper™

Bastion™

DeepSecure™