

MIMESweeper™ for Exchange

Award-winning MIMESweeper policy-based content security for internal email

Internal email has moved from a simple messaging medium to become a critical vehicle for distributing documents and other files. But just as it has accelerated the process of internal communications, it is now exposing organizations to a host of new threats. Internal users pose a significant security threat through malicious or purely accidental circulation of inappropriate emails content and attachments. The 2004 Information Security Breaches Survey from the Department of Trade and Industry (DTI) shows that around one third of security issues originate internally.

MIMESweeper for Exchange

MIMESweeper for Exchange allows organizations to protect against digital threats coming from internal email communication. These threats are the same as those faced on the SMTP gateway (e.g. virus infections, exposure to or circulation of profanity and other offensive content, distribution of confidential information, loss of network bandwidth and storage, and many others) and can be propagated by employees sending round jokes, MP3 files or defamatory emails. In addition, they may - unwittingly or not - upload a virus onto the corporate system from a disk or their laptop. All these threats can be detected and stopped through the implementation of MIMESweeper for Exchange.

MIMESweeper for Exchange comprises:

- MIMESweeper award-winning content analysis engine
- Web-based Report Center
- REMOTEmanager
- Personal Message Manager (PMM)
- Anti-spam Filter

The threat within: gateway security is not enough

While many threats originate from outside the organization, installing gateway protection does not ensure that the network and the business are completely safe from digital attacks or business threats leading to litigation.

Organizations are also under threat from viruses and illegal or inappropriate material entering a network via web access, CDs / floppy disks and laptops which are taken out of the office and then distributed to other users via internal email.

Furthermore, many organizations have either already implemented or are planning to implement web-based access to Outlook. This means that threats can be brought into the email system without going anywhere near an SMTP gateway solution.

The deliberate or accidental circulation to the wrong user of confidential information held by HR, sales, legal and research departments, is a major worry for all businesses today, especially with the introduction of new legislation like the Data Protection Act in Europe. It is therefore vital for organizations to be able to enforce policies that ensure sensitive data cannot be purposefully or accidentally emailed to unauthorized personnel. One obvious example is in the financial industry where legislation prevents buyers from sending information details to sellers. Another is personnel departments and ensuring personal details of employees, such as wages or disciplinary details are not accidentally or otherwise sent to someone who is not authorized to receive such information.

The Issues:

Security: Viruses, Trojans and malicious code can all be transmitted via internal email. With the vast majority of internal communications being carried out electronically, the chances of attacks on data integrity are increasing.

Productivity: As employees increasingly rely on email as the main communication vehicle, the volume of emails has grown exponentially. On average there is 8 times as much email sent internally as there is externally. Not only does this lead to time lost through the management of inboxes, but employees also use the system to share jokes and other non-business related material.

IT costs: In today's cost cutting culture, it is imperative that IT costs do not spiral due to uncontrolled email. Without filtering and analyzing your email traffic, can you be certain that the large amount of data being circulated around your network is business related?

Legal liability: The circulation of offensive or inappropriate content, copyrighted material and corporate confidential information can all lead to litigation and damage to reputation. The results of such litigation could cause irreparable damage to your organization.

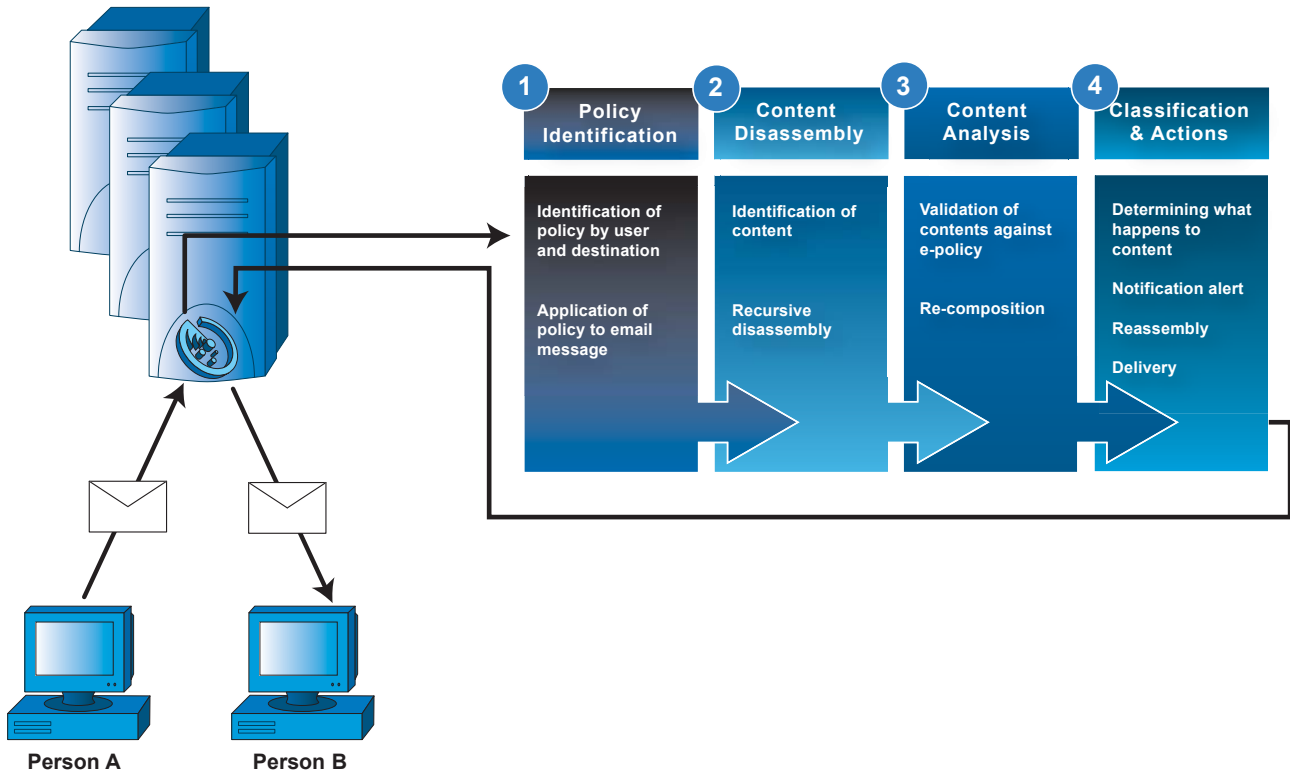
Compliance: Organizations face continuing changes in both legislation and market regulation. Your company is now more accountable for how information is stored, used and distributed - it is imperative that data is managed and controlled correctly.

Product Highlights:

- World's #1 email content security product
- Stops the spread of digital threats by internal email
- Prevents the distribution of viruses and inappropriate messages
- Web-based Report Center enables greater corporate access to information
- REMOTEmanager facilitates anytime, anywhere system administration

How Does it Work?

The Exchange Intercept Module intercepts all email on the Exchange Server before delivery, and then passes it on to MIMESweeper for processing.

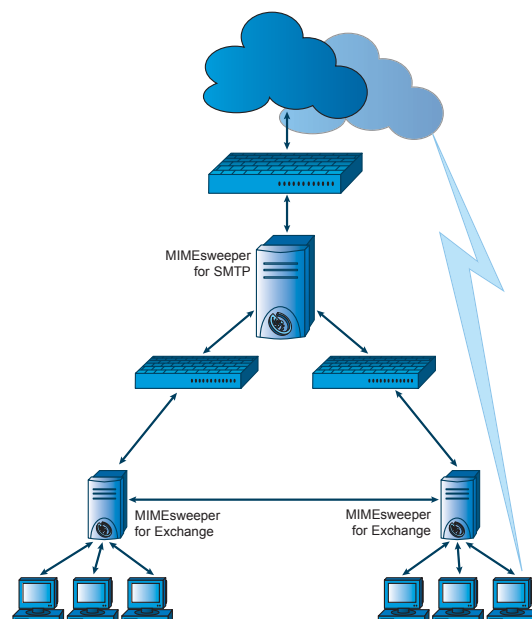


Deployment

MIMESweeper for Exchange can be deployed in a number of different architectures and alongside other MIMESweeper products, depending on the size and complexity of the internal email infrastructure.

The deployment of MIMESweeper for Exchange on multiple Microsoft Exchange servers prevents the distribution of threats between users in the same organization. MIMESweeper for SMTP managed as part of the perimeter security solution is then used to control inter-organizational issues such as spam and external denial of service attacks - protecting and enhancing the internal network resources by retaining inappropriate content at the network perimeter.

In organizations that are geographically dispersed, MIMESweeper for Exchange can be deployed to allow local autonomy for either definition of intra-organization communication or regional variations to the corporate policy.



Comprehensive Security

MIMESweeper for Exchange provides the answer to total email security. It combines the technical brilliance of Clearswift's MIMESweeper content security technology and management functionality to provide unbeatable protection against digital threats, both today and in the future. In addition, it significantly reduces the time and resource required to manage the email server.

MIMESweeper for Exchange enables an organization to implement email content security policies on Microsoft Exchange Server 2000/2003. It intercepts, analyzes and processes all messages routed through the Exchange Server according to your organization's policy.

Simplifying your Administration

Managing systems can be time consuming for IT departments. MIMESweeper for Exchange significantly reduces the time and effort needed to control internal messaging security.

REMOTEmanager is a web-based management and administration add-on tool that boosts MIMESweeper's extensive management capabilities for System Administrators. It enables administration tasks to be carried out remotely and by multiple users.

The Report Center within MIMESweeper tells you everything you need to know to make better management, capacity planning and security policy decisions. The information is presented in a wide range of pre-defined, graphical reports that simplify and help justify decision-making.

Total Content Security

As email and Internet usage continues to grow, an organization's 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 taking at least three layers of defense at the SMTP gateway to ensure against digital attacks:

Entry

- Firewalls - only have "block/allow" functions. SMTP and HTTP are in the "allowed" category
- Anti-virus software - protects against viruses, however can only react to known threats

Basic Security

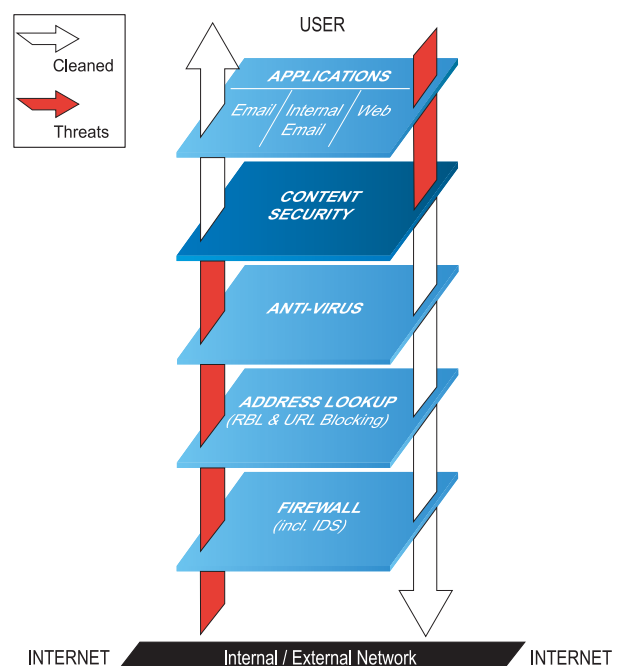
- Address Lookup - software designed to block access to traffic deemed a threat to company security according to a database of blacklisted addresses.

Complete Security

- Content Analysis - Software that scans content in real-time according to policy. Permits or denies access depending on analysis of file type, text, images and embedded code.

The data in the email message transfer is analyzed and evaluated in line with the organization's security policy, depending on sender-recipient route. Emails can be blocked based on file types, inappropriate text or offensive images.

Simply relying on the first layer will leave the organization open to a large number of digital threats and will not help to ensure that market rules are adhered to.



MIMESweeper™ for Exchange

E-Policy Based Content Security

MIMESweeper for Exchange enables organizations to enforce a comprehensive e-policy within a clearly defined framework. Once the policy had been established, and employees have been educated on what is or isn't acceptable use of email, organizations can then enforce e-policies consistently and uniformly utilizing this installed technology base.

MIMESweeper for Exchange provides a simple and intuitive 'Policy Manager' that allows different policies to be applied to different users at both an individual and group level. E-policy administration wizards easily guide System Administrators through the task of defining and implementing effective security policies.

Technical Requirements

- Windows 2000 Server (SP4 or higher) or Windows Server 2003
- Microsoft Exchange 2000 Server (SP3 or higher) or Exchange Server 2003 (SP1 or higher).
- Minimum recommendation Pentium™ III 800 MHz or equivalent
- 1 Gb free space on NTFS partition for installation
- 1 Gb free space in /temp directory
- 512 Mb memory

Why Clearswift?

Clearswift is the world's #1 in Content Security. We secure content, increase productivity, reduce IT costs, protect against digital attacks and create safer business environments by enforcing policies. With a growing user-base of more than 15,000 customers, 20 million users around the world depend on Clearswift for protection and peace of mind.

Contact Clearswift

United States

303 Twin Dolphin Drive, 6th Floor,
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 650 632 4601

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

Sweden

Frösundaviks allé 15, 4tr, SE-169 70 Solna
Tel: +46 8 50 90 40 78 | Fax: +46 8 655 26 10

Japan

Eisho Takanawadai Bldg 6F, 2-11-8, Minato-ku Shiroganedai
Tokyo-to, 108-0071
Tel: +81 (3) 5423 8171 | Fax: +81 (3) 5423 1274

MIMESweeper™ for SMTP

MIMESweeper™ for Web
URL Filter
Reporting

MIMESweeper™ for Exchange

MIMESweeper™ for Domino
e-Sweeper™
IMAGEmanager™