

## MIMESweeper™ for SMTP 5.0

# Die weltweit führende Content Security-Lösung für Email

## Schützt gegen Spam und Viren und alle anderen Email-Gefahren

Nicht nur die Zahl der digitalen Attacken nimmt kontinuierlich zu, sie entwickeln sich auch ständig weiter. Daher ist es für Unternehmen unerlässlich, sich gegen neuartige Angriffe zu schützen, noch bevor Entwickler von Anti-Viren- und Sicherheitssoftware Patches oder Updates gegen neue Bedrohungen zur Verfügung stellen. Durch ineffizientes Patch-Management können Virenautoren den Vorteil so genannter „Zero-Day-Attacken“ nutzen und somit Schäden in Millionenhöhe anrichten.

Zudem gewinnen Themen wie unangemessene Inhalte, gesetzliche Auflagen und Richtlinien sowie Geheimhaltung immer mehr an Bedeutung für Unternehmen und sollten nicht unterschätzt werden.

IT-Manager nehmen mittlerweile Abstand vom Einsatz von Einzellösungen und setzen heute vermehrt umfassende, unternehmensweite Content Security-Lösungen ein. Sie fordern dabei Lösungen mit niedrigen TCO (Total Cost of Ownership) sowie geringen Anforderungen an Bandbreite und Speicherplatz.

Clearswift weiß, dass Unternehmen – gleich welcher Größe – keine Risiken bei der Sicherheit ihrer unternehmenskritischen Email-Applikationen eingehen können. Sie müssen sich daher auf die besten Lösungen verlassen können. Seit der Einführung im Jahr 1995 gilt MIMESweeper for SMTP als eine der weltweit leistungsfähigsten Content Security-Lösungen.

## MIMESweeper for SMTP

MIMESweeper for SMTP ist eine der am weitesten entwickelten und vielseitigsten Content Security-Lösungen. Sie erfüllt sämtliche Anforderungen mittelständischer und großer Organisationen aus den unterschiedlichsten Bereichen wie Finanzen, Behörden, Hersteller, Einzelhändler und High-tech-Industrie.

Im Gegensatz zu anderen Sicherheitslösungen, die lediglich Schutz gegen ein oder zwei Gefahren bieten (z.B. spezielle Anti-Spam-, Anti-Viren oder Anti-Spyware-Lösungen), bietet MIMESweeper for SMTP Schutz gegen alle Content Security-Risiken – bevor diese den Geschäftsbetrieb beeinträchtigen.

MIMESweeper for SMTP ermöglicht automatische Updates zum Schutz gegen „Zero-Day-Attacken“. Der automatische ThreatLab™-Service, der eine Überprüfung von Phrasen, Scripten und Dateiprüfsummen beinhaltet, führt Software-Updates durch, ohne dass man selbst Hand anlegen muss. So erhöht MIMESweeper nicht nur die Sicherheit durch zusätzlichen und zeitnahen Schutz gegen neuartige Angriffe, sondern reduziert auch den Zeit- und Kostenaufwand für den Download von Updates.

MIMESweeper for SMTP bietet

- **Policy-basierte Content Security**
  - Hierarchische, rollenbasierte Sicherheit
  - Personal Message Manager
- **Erweitertes Gefahrenmanagement**
  - Proaktive, automatische Updates
  - Mehrstufige Anti-Spam-Lösung
  - Fortschrittliche Viren-Prüfung
- **Umfassendes Remote-Management und -Reporting**
  - Sicheres Policy-Management und Policy-Administration
  - Zentrale Policy-Konfiguration über alle Server
  - Konsolidiertes Quarantänenmanagement
  - Mehrere Administrator-Accounts für gleichzeitigen Zugriff

### Die Kernpunkte:

**Sicherheit:** Viren, Trojaner und bösartiger Programmcode können durch Emails übertragen werden. Da heute der größte Teil der geschäftlichen Kommunikation über elektronische Medien erfolgt, ist die Gefahr digitaler Angriffe groß.

**Produktivität:** Produktivitätsverluste entstehen nicht nur durch Email-Missbrauch oder unangemessene Kommunikation unter Mitarbeitern. Oftmals ist Spam die Ursache. Mitarbeiter müssen sich im Durchschnitt täglich 10 Minuten und IT-Mitarbeiter bis zu 43 Minuten mit Spam beschäftigen.

(Quelle: IDC, 2004)

**Haftungsrisiken:** Die Verbreitung beleidigender oder unangemessener Inhalte, urheberrechtlich geschützten Materials sowie vertraulicher Unternehmensinformationen per Email kann zu Haftungsrisiken und Rufschädigung führen.

**Gesetzeskonformität:** Unternehmen sehen sich einer stetig steigenden Anzahl gesetzlicher Auflagen und Richtlinien gegenüber und sind für die Speicherung, Verwendung und Weitergabe von Informationen verantwortlich. Bei Missachtung dieser Auflagen drohen empfindliche Geldstrafen sowie Strafverfolgung und Zivilprozesse.

### Produkt-Highlights:

- Weltweit führende Content Security-Lösung
- Schutz gegen „Zero-Day-Attacken“ durch automatische Updates
- Verhindert das Eindringen von Viren
- Wehrt 98 % der Spam-Mails ganz ohne falsche Treffer (false positives) ab
- Proaktive Spam- und Threat-Updates halten Systeme auf dem neuesten Stand
- Hoch skalierbare Lösung mit Unterstützung von bis zu vier Servern
- Komfortable Verwaltung für 50 oder 100.000 Anwender
- Hervorragende rollenbasierte Sicherheitsfunktionen ermöglichen die Durchsetzung selbst extrem detaillierter Richtlinien
- Komfortable Policy-Assistenten
- Intuitive Web-basierte Managementoberfläche
- Personal Message Manager ermöglicht Anwendern die Verwaltung ihrer Emails im Quarantänebereich
- Web-basiertes Report Center mit mehr als 20 vorkonfigurierten Berichten
- Funktionen für Bildanalyse/-erkennung

## Niedrigere TCO und schnellerer ROI (Return On Investment)

Die TCO von MIMESweeper sind gering und der Einsatz entlastet die Mitarbeiter der IT-Abteilung dank einer innovativen Managementoberfläche erheblich. Das System ermöglicht die Verwaltung der SMTP-Gateways über eine Web-basierte Managementkonsole. Somit werden Verwaltungsaufgaben vereinfacht und es wird sichergestellt, dass Sicherheitsrichtlinien organisationsweit durchgesetzt werden.

Weiterhin können Organisationen durch die automatische Kompression von Dateien Bandbreiten- und Speicherkosten, die durch ein großes Email-Volumen entstehen, erheblich reduzieren.

## Eine Lösung, die gegen ALLE digitalen Gefahren schützt

### MIMESweeper Virenschutz – gegen bekannte und unbekannte Gefahren

Studien von Clearswift haben gezeigt, dass Unternehmen Computerviren mehr als alle anderen digitalen Gefahren fürchten.

MIMESweeper for SMTP ist auf Kompatibilität mit dem Anti-Viren-Tool Ihrer Wahl ausgerichtet. Die Lösung fängt Daten am Gateway ab und zerlegt diese, bevor sie zur Virenprüfung und -beseitigung an die Anti-Viren-Lösung weitergeleitet werden. Dies gewährleistet den optimalen Schutz gegen bekannte Viren.

Zwischen dem ersten Auftauchen einer neuen Gefahr und der Bereitstellung von Patches oder Updates seitens der Anbieter von Anti-Viren- und Sicherheitslösungen entsteht ein Zeitfenster, in dem die Systeme angreifbar sind. Gerade hierauf ist MIMESweeper for SMTP spezialisiert und fängt auch Viren, Würmer und Trojaner ab, die Anti-Viren-Softwareherstellern noch nicht bekannt sind. Somit wird die Integrität des gesamten Netzwerks gewährleistet.

## Eine Lösung, die gegen ALLE Geschäftsbedrohungen schützt

### Produktivitätsverlust

MIMESweeper for SMTP verhindert den Email-Missbrauch, sodass die Systemressourcen des Unternehmens nicht durch belanglose oder unerwünschte Emails verschwendet werden. Die Lösung verfügt über umfangreiche Reporting-Tools, mit denen Systemadministratoren die tägliche Email-Nutzung, Missbräuche sowie Trends im Blick haben und zukünftige Anforderungen identifizieren können.

### Gesetzeskonformität und Haftungsrisiken

Der Umfang gesetzlicher Vorgaben für Unternehmen nimmt kontinuierlich zu: Sarbanes-Oxley-Act, Gramm-Leach-Bliley, HIPAA, SEC, Basel II, Data Protection Act etc. Darüber hinaus haben Unternehmen ihren Mitarbeitern, Partnern und Kunden gegenüber eine Sorgfaltspflicht. Werden diese mit illegalen oder anstößigen Inhalten (Pornografie, Rassismus oder Beleidigungen) behelligt, kann dies kostspielige Klagen gegen das verantwortliche Unternehmen zur Folge haben. Der Verlust vertraulicher Informationen und geistigen Eigentums stellt eine weitere Gefahr dar, die hohe Kosten verursachen und den Ruf des Unternehmens ruinieren kann.

Durch den Einsatz von MIMESweeper for SMTP können Unternehmen Haftungsrisiken vermeiden und gesetzliche Auflagen erfüllen. Dank der leistungsfähigen, richtlinienbasierten Content Security-Engine werden je nach Anforderung sowohl komplexe als auch einfache Richtlinien unterstützt. Da sämtlicher Datenverkehr am SMTP-Gateway genau überprüft wird, können alle versehentlichen oder absichtlichen Verstöße vermieden werden, bevor es zu Problemen kommt.

### MIMESweeper Schutz gegen Spam – umfassende und anpassungsfähige Sicherheitsfunktionen

MIMESweeper for SMTP 5.0 beinhaltet eine integrierte, mehrstufige Anti-Spam-Komponente, die drei State-of-the-Art-Technologien zu einer effizienten „Knowledge Engine“ kombiniert – Software, die im laufenden Betrieb lernt, wie sie das jeweilige Unternehmen optimal schützen kann. Die Lernfähigkeit dieser Software bietet Unternehmen die Möglichkeit, Anti-Spam-Profilen zu generieren, die so individuell wie ihre Mitarbeiter sind. Eingehende Emails, die aktuellen Spam-Profilen entsprechen, werden von dem Filter auf Basis der Anti-Spam-Policy sofort aussortiert, sodass unerwünschte Nachrichten nicht in das Unternehmensnetzwerk gelangen können.

Direkt nach der Installation erkennt MIMESweeper 98 Prozent der Spam-Mails und verhindert durch den Einsatz von Personal Message Manager falsche Treffer.



## Hierarchische, rollenbasierte Content Security

Eine wesentliche Voraussetzung für die Content-Analyse ist die Definition von Richtlinien, in denen festgehalten ist, welche Nutzung von Email- und Internetsystemen für Mitarbeiter eines Unternehmens legitim ist. In diesen Richtlinien müssen mögliche Gefahren, gesetzliche Auflagen und Bestimmungen sowie individuellen Rollen und Anforderungen von Mitarbeitern an die Systeme berücksichtigt werden.

MIMESweeper for SMTP unterstützt unternehmenseigene Sicherheitsrichtlinien und verfügt über einen leistungsstarken, rollenbasierten Sicherheitsansatz. Die meisten Lösungen von Mitbewerbern ermöglichen lediglich das Aktivieren oder Deaktivieren von Funktionen. MIMESweeper for SMTP hingegen verwirklicht ein hierarchisches Konzept, das Unternehmen die Anwendung verschiedener Sicherheitsarten und -levels für einzelne Benutzer ermöglicht.

## Bemerkenswert skalierbar

Im Gegensatz zu vielen anderen Lösungen ist MIMESweeper for SMTP eine Langzeitinvestition und stellt gewissermaßen das Rückgrat der Email-Sicherheit dar. Diese Lösung kann individuell an die wachsenden Anforderungen von Unternehmen angepasst werden und eignet sich gleichermaßen für 50 und 100.000 Mitarbeiter. Dank der hohen Skalierbarkeit von MIMESweeper for SMTP können Kunden sicher sein, dass sie in eine Lösung investiert haben, die sie jetzt und auch in Zukunft schützt.

## Wie es funktioniert

MIMESweeper for SMTP analysiert alle über das Gateway ein- und ausgehenden Emails in vier Schritten:



## Einfach zu verwalten

Management und Administration von Sicherheitssystemen stellen häufig zeitaufwändige Belastungen für IT-Mitarbeiter dar. Die intuitive, Web-basierte Managementoberfläche von MIMESweeper ermöglicht mehreren Administratoren gleichzeitig ein effizientes, konsolidiertes Management von einem Standort aus und führt dadurch zu erheblicher Zeitersparnis. MIMESweeper for SMTP umfasst fünf verschiedene Managementbereiche:

- **Systems Center** – ermöglicht Administratoren die Verwaltung aller Dienste, die auf jedem Host eingesetzt werden und eine Statusüberprüfung von Emails
- **Security Center** – hier ist definiert, welche Aufgaben und Zuständigkeiten den Administratoren zugeteilt sind
- **Message Center** – hier wird der Hauptteil der täglichen Aufgaben durchgeführt. Dieses Center bietet einen einheitlichen Überblick über die verschiedenen Quarantänebereiche sowie Nachrichtenordner und erleichtert somit den Aufwand für die Verwaltung mehrerer Server
- **Report Center** – dieser Bereich bietet Administratoren Zugriff auf 20 vorkonfigurierte Berichte und effiziente Assistenten, mit denen maßgeschneiderte Berichte erstellt werden können
- **System Health** – eine einzige Webseite, die Überblick über alle laufenden Systeme der gesamten Konfiguration bietet. Diese Seite gibt Aufschluss über den Nachrichtenfluss, die Anzahl der unter Quarantäne gestellten sowie der weitergeleiteten Nachrichten und Informationen zu aktuellen Trends (wie z.B. zu- oder abnehmende Warteschlangen)

Der intelligente Ansatz von MIMESweeper zur Systemverwaltung ermöglicht die hierarchische Verteilung von Aufgaben an mehrere Administratoren. So können IT-Manager spezifische Aufgaben wie Serverüberwachung, Bearbeitung bestimmter Quarantänebereiche und Reporting an entsprechende Administratoren oder Abteilungen übertragen. Dadurch lässt sich der Zeitaufwand für das Management festgehaltener Emails erheblich reduzieren.

MIMESweeper for SMTP ist nicht nur eine leistungsfähige Sicherheitslösung, sondern auch ein umfassendes Management-Tool.

## Message Management

Das steigende Spam-Volumen erfordert viel Zeitaufwand seitens der IT-Abteilung. Nach Angaben des Marktforschungsunternehmens IDC müssen IT-Mitarbeiter im Durchschnitt täglich 43 Minuten kostbare Zeit für die Verwaltung von Spam aufwenden. Und dabei geht es nahezu ausschließlich um die Überprüfung blockierter Nachrichten auf Spam und gegebenenfalls die Freigabe relevanter Geschäfts-Emails, die fälschlicherweise als Spam klassifiziert wurden.

Mit dem Personal Message Manager können die Anwender selbst festlegen, ob ihre unter Quarantäne gestellten Emails tatsächlich als Spam einzustufen sind. Diese Schlüsselfunktion entlastet die IT-Abteilung und stellt sicher, dass Spam-Emails noch präziser identifiziert werden.

## Email-Profile verstehen

Eine effiziente IT-Sicherheitsrichtlinie kann nur implementiert werden, wenn die Art und Weise der Email-Nutzung sowie die Gefahren, denen ein Unternehmen ausgesetzt ist, bekannt sind. Das Report Center verfügt über umfassende, vordefinierte Berichtsfunktionen, die über eine sichere Verbindung von jedem Standard-Internetbrowser eingesehen werden können. Die detaillierten und übersichtlichen grafischen Berichte bieten Mitarbeitern folgende Vorteile:

- Darstellung des ROI durch grafische Berichte
- exakte Analyse des gesamten Email-Verkehrs
- Audit- und Berichtsfunktionen zur Identifikation von Spitzenlastzeiten des Email-Verkehrs
- bessere Kapazitätsplanung für mehr Leistung bei niedrigeren Kosten
- Feinabstimmung der Richtlinien entsprechend den aufgetretenen Gefahren
- Übersicht über die in den Emails enthaltenen Datentypen



# MIMESweeper™ for SMTP 5.0

## Optionale Funktionen

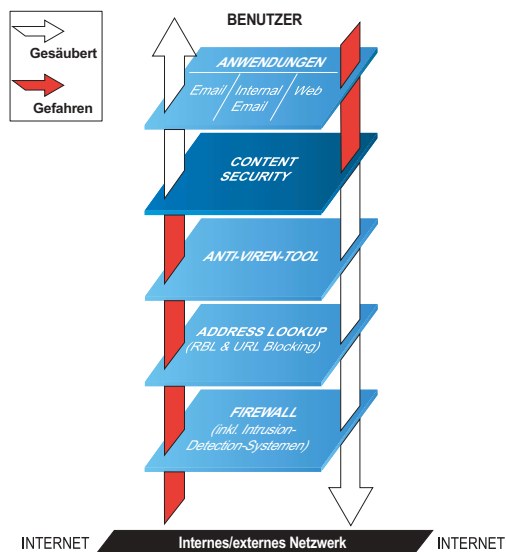
### IMAGEmanager

Durch Verwendung ausgefeilter Analysealgorithmen für Bilder kann MIMESweeper pornografische und andere unangemessene Bilder, die in Emails eingebettet oder angehängt sind, identifizieren und blockieren. Darüber hinaus können Unternehmen die Datenbank durch eigene Bilder ergänzen, um sicherzustellen, dass vertrauliche Bildinhalte wie Pläne und Entwürfe beim Versand automatisch erkannt und blockiert werden.

### Content Security Total

Die Nutzung von Email und Internet nimmt stetig zu. Allerdings ist zu beachten, dass Sicherheitssysteme immer nur so stark sind wie ihre schwächste Komponente. Fehler können zu immensen Kosten führen. Viele Unternehmen setzen daher zunehmend mehrstufige Sicherheitslösungen ein. Ein derartiger Ansatz erfordert zusätzliche und ergänzende Sicherheits-Tools auf mehreren Ebenen für alle Gateways und Protokolle.

Clearswift ist überzeugt, dass mindestens drei Sicherheitsebenen am SMTP-Gateway erforderlich sind, um Schutz gegen digitale Angriffe zu gewährleisten.



## Technische Voraussetzungen

### Betriebssystem

- Windows XP (SP1-unterstützt, aber nicht empfohlen)/2000 Server (SP4)/2003 Standard oder Enterprise (englisch, französisch oder deutsch)

### Hardware

- Pentium III 800 MHz oder gleichwertig (Mindestempfehlung bei geringem Email-Durchsatz, abhängig von Konfiguration, Benutzeranzahl und Email-Volumen)
- 10 GB freier Festplattenspeicher für die Installation (NTFS-Partition)
- 10 GB freier Festplattenspeicher für das temp-Verzeichnis
- 1 GB Arbeitsspeicher

### Software

- SQL 2000, MSDE, Oracle 9 für Reporting
- Microsoft Active Directory 200x/Exchange 5.5 und Domino Directory Server
- Microsoft Data Access Components 2.8 oder höher
- Microsoft CDO for Windows 2.0 (Bestandteil von Windows 2000)
- Internet Information Services (IIS) mit ASP.NET-Unterstützung (letzte IIS Sicherheitspatches von Microsoft empfohlen)

## Was spricht für Clearswift?

Clearswift ist weltweit die #1 in Content Security. Wir sorgen für sichere Inhalte und schützen gegen digitale Angriffe. Mit unseren Produkten lassen sich Policies zur Produktivitätssteigerung, IT-Kostensenkung und Gestaltung einer sicheren Geschäftsumgebung umsetzen. Bei wachsender Anwenderbasis bietet Clearswift 15.000 Kunden und 20 Millionen Nutzern weltweit Schutz und unbeschwertes Arbeiten.

## Kontakt Clearswift

### Deutschland

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

### USA

15500 SE 30th Place, Suite 200,  
 Bellevue, Washington, 98007  
 Tel. +1 425 460 6000 | Fax: +1 425 460 6185

### Großbritannien

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

### Australien

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

### Schweden

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™**