



# GFI MailEssentials

for Exchange/SMTP/Lotus

Spam-Filter und E-Mail-Management für Exchange/SMTP/Lotus Notes

Effizient und leistungsstark: GFI MailEssentials bietet Spammern keine Chance, ihre unerwünschten Werbebotschaften ins Ziel zu bringen. Schon mehr als 80.000 Kunden weltweit vertrauen auf die mit über 60 Auszeichnungen prämierte Nummer 1 unter den Anti-Spam-Lösungen.

Ausgestattet mit gleich zwei Schutz-Engines, wehrt GFI MailEssentials Spam mit bisher unerreichter Zuverlässigkeit ab, ohne umfassende Voreinstellungen vornehmen zu müssen. Ob mit einer der branchenweit höchsten Erkennungsraten von über 98 % oder marktweit günstigsten Preisen – die Messaging-Lösung weiß in jeder Hinsicht zu überzeugen.

Jetzt neu ab Version 14: die ergänzende Anti-Spam-Engine SpamRazer für doppelten Schutz. Dank häufiger automatischer Updates kommt der intuitive SpamRazer ohne Konfigurierung und Lernphase aus. So lassen sich von Anfang neueste Spam-Angriffe wie NDR- (Non-Delivery-Report), CNN- und MSNBC-Spam sowie andere künftige Bedrohungen effizient abwehren. Zusätzlich sorgen die Filterung per IP-Reputation, Bayes'sche Analyse und andere fortschrittliche Sicherheitsmodule für eine bestmögliche Erkennung und Blockierung unerwünschter Mitteilungen. Nicht zuletzt überzeugt GFI MailEssentials mit einer unübertroffenen geringen Anzahl von Fehlalarmen bei der Überprüfung der E-Mail-Korrespondenz.

GFI MailEssentials erkennt und blockiert zudem betrügerische Phishing-E-Mails und erweitert die Funktionalität von Mailservern mit Verwaltungs-Tools wie POP3-Downloader, Server-basierte Auto-Replies, E-Mail-Überwachung, Internet-Mail-Berichterstellung, Listen-Server und Disclaimer.

## Vorteile

### Warum gerade GFI MailEssentials als Spam-Filter?

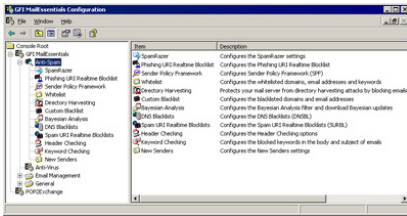
- Beliebteste Anti-Spam-Lösung mit konkurrenzlosem Preis-Leistungsverhältnis – erhältlich ab netto 186,40 €
- Im Einsatz bewährt: über 80.000 Installationen und mehr als 60 Auszeichnungen
- Bietet gleich zwei Anti-Spam-Engines für eine optimale Spam-Erkennungsrate von über 98 %
- Besticht mit einem Minimum an Fehlalarmen
- Unterstützt die branchenführenden Messaging-Plattformen Microsoft Exchange 2000, 2003, 2007 und Lotus Domino

### ■ SpamRazer – zusätzlicher Schutz vor Spam-Mails

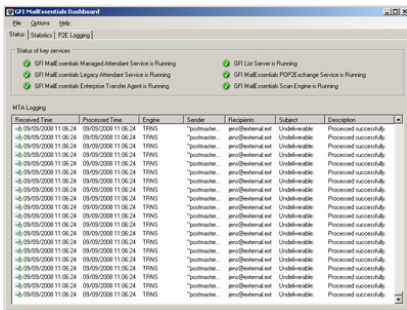
SpamRazer als ergänzende Anti-Spam-Engine sorgt in der neuesten Version von GFI MailEssentials für doppelten Schutz. Dank häufiger automatischer Updates kommt das intuitive Abwehrmodul ohne Konfigurierung und Lernphase aus. So lassen sich von Anfang an aktuelle Spam-Angriffe wie NDR- (Non-Delivery-Report), CNN- und MSNBC-Spam sowie viele andere Bedrohungen effektiv blockieren. Die Engine nimmt ihre Arbeit ohne weitere Voreinstellungen auf – selbst bei neuen Spam-Wellen müssen Administratoren keine Anpassungen vornehmen. Zusätzlich sorgen die Filterung per IP-Reputation, Bayes'sche Analyse und andere fortschrittliche Abwehr-Technologien für eine Spam-Erkennungsrate von über 98 %. Präzise Analysefunktionen garantieren ein branchenweit führendes Minimum an Fehlalarmen, um zu gewährleisten, dass erwünschte Nachrichten nicht versehentlich gelöscht werden.

### ■ Echtzeit-Dashboard für präzisen Überblick

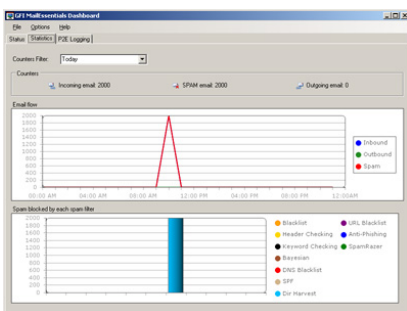
Administratoren können sich mit einem Blick auf das Echtzeit-Dashboard über den Status der Sicherheitslösung und die vom Mailserver verarbeiteten Nachrichten informieren. Die Anzeige gibt Aufschluss über den Zustand der wichtigsten Dienste von GFI MailEssentials, liefert Statistiken zur E-Mail-Übertragung sowie zu abgewehrtem Spam und informiert über POP2Exchange-Prozesse.



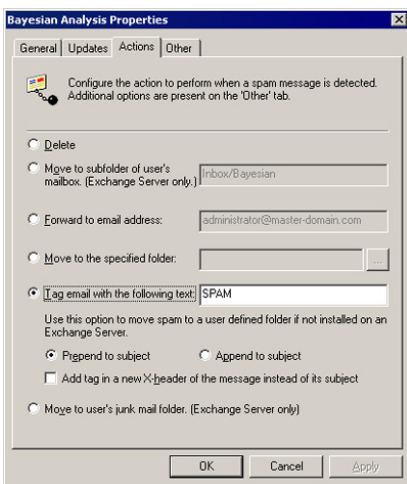
Spam-Filter-Varianten



Statusansicht des Echtzeit-Dashboards



Statistikansicht des Echtzeit-Dashboards



Umfangreiche Optionen zur Spam-Bekämpfung

## ■ Ressourcenschonende Implementierung

Einbindung in die Exchange-Server-Umgebung und Kontrolle erfolgen bereits auf Ebene des SMTP-Protokolls. Mailserver müssen Nachrichten nicht vollständig abrufen, damit GFI MailEssentials feststellen kann, ob es sich um Spam oder eine erwünschte E-Mail handelt. Bandbreite und Prozessorleistung lassen sich hierdurch noch effizienter nutzen.

## ■ Bericht zum Spam-Aufkommen

Mitarbeiter können per Reporting-Funktion täglich über die unter ihrer Adresse eingegangenen Nachrichten informiert werden, samt Aufschlüsselung in legitime E-Mails und blockierten Spam. Diese Momentaufnahme hält Anwender stets über die Effizienz der Anti-Spam-Engines und den Spam-Anteil ihrer empfangenen Korrespondenz auf dem Laufenden. Zusätzlich erhalten sie eine vollständige Übersicht zu sämtlichen als Spam identifizierten und blockierten Mitteilungen.

## ■ Abwehr von schwer erkennbarem Unzustellbarkeits-, MSNBC- und CNN-Spam

Viele Spammer haben tausende Rechner argloser User unter ihrer Kontrolle ("Zombie-PCs"), die sie zum Massenversand von Nachrichten missbrauchen. Mit Hilfe des Botnet/Zombie-Checks von GFI MailEssentials lässt sich schwer identifizierbarer Attachment-Spam wie Bilder-, PDF-, Excel- und ZIP-Spam abwehren. Unerwünschte E-Mails werden rasch und zuverlässig herausgefiltert – bei einer sehr geringen Anzahl an Fehlalarmen. Gleich zwei Anti-Spam-Filter und leistungsstarke Technologien wie Bayes'sche Analyse und IP-Reputation dämmen die Flut an NDR-(Non-Delivery-Report), CNN-, MSNBC- und zahlreichen anderen Spam-Varianten ein, um mehr über Attachment-Spam zu erfahren oder über NDR-Spam.

## ■ Server-basierte Abwehr von Spam- und Phishing-E-Mails

GFI MailEssentials wird auf Server-Basis eingesetzt und auf dem Mailserver oder Gateway installiert. Der Einsatz und die lästige Administration Desktop-gestützter Produkte zur Spam- und Phishing-Abwehr ist nicht länger notwendig. Beim Schutz auf Desktop-Basis müssen Anwender sich beispielsweise mit dem Erstellen von Anti-Spam-Regeln auskennen und diese danach auch weiterhin regelmäßig aktualisieren – eine große Herausforderung. Zudem sind dabei die Server-Nachrichtenspeicher auch weiterhin der großen Flut von Spam-Mitteilungen ausgesetzt.

## ■ Bayes'sche Filtertechnologie

Die Bayes'sche Filtertechnologie wird von führenden Experten und Fachpublikationen als beste Methode zur Spam-Abwehr empfohlen. Spam wird anhand statistischer Berechnungen identifiziert, die bekannte Spam-Mitteilungen und erwünschte Nachrichten ("Ham") berücksichtigen. Der lernfähige Filter ist anderen Anti-Spam-Lösungen überlegen, da er nicht nur nach Stichwörtern sucht oder bei der Blockierung lediglich auf heruntergeladene Spam-Signaturen vertraut. Zur Erkennung und Abwehr unerwünschter Mitteilungen setzt der Bayes'sche Filter von GFI spezielle mathematische Formeln und einen Datenbestand ein, der direkt an Ihr eigenes Mail-System angepasst wird. GFI erfasst hierfür fortlaufend neue Spam-Daten, die GFI MailEssentials selbstständig herunterlädt. Alle Ham-Daten werden wiederum automatisch über ausgehende E-Mails ermittelt. Der Bayes'sche Filter rekonfiguriert sich daher kontinuierlich – Spammer können diesen individuellen Schutz nicht überwinden. Schon nach einer zweiwöchigen Lernphase ist eine Spam-Erkennungsrate von über 98 % möglich. Die Bayes'sche Filtermethode hat unter anderem folgende Vorteile:

- Überprüft die Mitteilung als Ganzes und erkennt Spam nicht nur über Stichwörter/bekannte Spam-Signaturen
- Lernt von ausgehenden Mitteilungen (Ham), um Fehlalarme zu reduzieren
- Passt sich durch Berücksichtigung neuer Spam-/Ham-Mitteilungen kontinuierlich an
- Stellt Unternehmen einen eigenen Datenbestand zur Spam-Abwehr bereit, der einen individuellen und daher unüberwindbaren Schutz bietet
- Kann für mehrere Sprachen eingesetzt werden

## ■ Regelmäßige Aktualisierung der Spam-Profil-Datenbank

GFI MailEssentials kann die Spam-Profil-Datenbank des Bayes'schen Filters über Update-Downloads von der GFI-Website aktualisieren. Dadurch werden immer die neuesten Spam-Varianten und -Techniken erkannt. Die Spam-Profil-Datenbank von GFI wird in Zusammenarbeit mit mehreren Organisationen, die Spam-Mitteilungen erfassen und darüber informieren, stets auf einem aktuellen Stand gehalten.

### ■ Schutz vor betrügerischen Phishing-E-Mails

Das Anti-Phishing-Modul schützt vor Gefahren, die von speziell präparierten, betrügerischen E-Mails ausgehen. Die Erkennung erfolgt über eine fortlaufend aktualisierte, spezielle Phishing-Datenbank – hierdurch lassen sich selbst die neuesten Phishing-Varianten abwehren. Zusätzlich wird in jeder empfangenen E-Mail nach Begriffen gesucht, die in typischen Phishing-E-Mails verwendet werden.

### ■ Verschieben von Spam in Benutzer-Ordner für Junk-E-Mail

GFI MailEssentials lässt Sie flexibel festlegen, wie mit Spam-Nachrichten zu verfahren ist. Spam kann gelöscht, in einen Ordner verschoben sowie an eine öffentliche E-Mail-Adresse, einen Öffentlichen Ordner oder an einzelne, spezielle Ordner (z. B. "Junk-Mail-Ordner") im Empfänger-Posteingang weitergeleitet werden. Anwender können E-Mails, die als Spam klassifiziert wurden, somit leichter überprüfen.

### ■ Listen-Server für Newsletter und Diskussionslisten

Unternehmens-Newsletter lassen sich optimal mit Hilfe eines Listen-Servers verschicken, der das Abonnieren von Mitteilungen und deren Abbestellung (durch Anti-Spam-Regelungen vorgeschrieben) automatisiert. Der Einsatz von Listen-Servern ist bislang jedoch mit hohen Kosten, einem großen Administrationsaufwand und der fehlenden Integrationsmöglichkeit mit Microsoft Exchange Server verbunden gewesen. GFI MailEssentials hingegen ist nahtlos in Exchange eingebunden und kann Microsoft Access oder Microsoft SQL Server als Datenbank-Backend nutzen. Als Mailing-Listen werden sowohl Newsletter als auch Diskussionslisten unterstützt.

### ■ Einfache Konfigurierung des Bayes'schen Filters mit Hilfe von Öffentlichen Ordnern

Die Bayes'sche Anti-Spam-Engine lässt sich auch mühelos per Drag-and-Drop konfigurieren: Spam oder Ham ist lediglich in die entsprechenden Öffentlichen Ordner zu verschieben. So lernt GFI MailEssentials, noch besser zwischen erwünschten und unerwünschten Mitteilungen zu unterscheiden. Um Missbrauch zu verhindern, ist es Systemverantwortlichen auch hier möglich, die Verwendung dieser Funktion über Richtlinien für Öffentliche Ordner einzuschränken.

### ■ Erweiterung von Blacklists oder Whitelists über Öffentliche Ordner

Anwender können einen E-Mail-Absender als erwünscht bzw. unerwünscht klassifizieren, indem dessen Mitteilung einfach per Drag-and-Drop in den entsprechenden Öffentlichen Ordner verschoben wird. Hierdurch können Benutzer aktiv eingreifen und den Administrationsaufwand verringern. Um Missbrauch zu verhindern, ist es Systemverantwortlichen auch hier möglich, die Verwendung dieser Funktion über Richtlinien für Öffentliche Ordner einzuschränken.

### ■ Analyse des E-Mail-Headers und Stichwort-Kontrolle

GFI MailEssentials führt eine intelligente Analyse des E-Mail-Headers durch und identifiziert Spam auch über die Informationen des Nachrichtenfelds. Auf diese Weise werden unter anderem gefälschte Header, verschlüsselte IPs, Spam-Mutationen und von ungültigen Domänen verschickte Spam-Mitteilungen erkannt. Zusätzlich zur Analyse des E-Mail-Headers lassen sich Spam-typische Begriffe für die Stichwortsuche festlegen.

## Systemanforderungen

- Microsoft Windows Server 2000/2003/2008 (Professional, Server oder Advanced Server) oder Windows XP Professional
- Installierter IIS5 SMTP-Dienst als SMTP-Relay zum Mailserver
- Microsoft Exchange Server 2007, 2003, 2000, 5.5, 5 oder 4, Lotus Domino oder andere gängige SMTP-/POP3-Mailserver
- Für den Listen-Server ist Microsoft Message Queuing Services (MSMQ) erforderlich
- Microsoft .NET Framework 2.0

## Auszeichnungen



Ihre Testversion steht unter <http://www.gfisoftware.de/de/mes/> zum Download bereit!

GFI Software  
Magna House, 18 – 32 London Road  
Staines, Middlesex  
TW18 4BP  
UK  
Tel +44 (0) 870 770 5370  
Fax +44 (0) 870 770 5377  
sales@gfi.co.uk

GFI Software  
15300 Weston Parkway  
Suite 104  
Cary, NC 27513  
USA  
Tel +1 (888) 243-4329  
Fax +1 (919) 379-3402  
sales@gfiusa.com

GFI Asia Pacific Pty Ltd  
83 King William Road  
Unley 5061  
South Australia  
Tel +61 8 8273 3000  
Fax +61 8 8273 3099  
sales@gfiap.com

GFI Software  
GFI House  
San Andrea Street  
San Gwann SGN 1612  
Malta  
Tel +356 2205 2000  
Fax +356 2138 2419  
sales@gfi.com

Microsoft  
GOLD CERTIFIED  
Partner

GFI  
www.gfi.com