

# GFI MailSecurity

Virenschutz, Inhaltsrichtlinien, Exploit-Erkennung und Trojaner-Abwehr für E-Mails

- **Führende** Multi-Engine-Virenabwehr
- Über **30.000** Kunden
- Konkurrenzloses Preis-Leistungsverhältnis
- Hervorragender Schutz

## Die führende KMU-Lösung zur Abwehr von E-Mail-Gefahren mit bis zu 5 Virenscannern

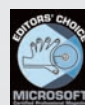
Die Bedrohung von Unternehmensnetzwerken durch Viren und Exploits ist weiterhin präsent – und wächst zudem beständig. Täglich werden neue Schädlinge und Varianten bereits bekannter Malware entdeckt. Abwehrlösungen mit nur einer einzigen Antiviren-Engine bieten schon längst keinen ausreichenden Schutz mehr, ob auf Server- oder Workstation-Ebene. Umfassendere und zuverlässigere Verteidigungsmaßnahmen sind erforderlich: GFI MailSecurity überprüft mit bis zu fünf Antiviren-Engines eingehende elektronische Post bereits auf dem E-Mail-Server auf Gefahren.

Die Vorteile des Einsatzes mehrerer Scan-Lösungen:

- Verkürzung der durchschnittlichen Wartezeit bei Signatur-Updates durch schnellstmöglichen Erhalt von Aktualisierungen
- Kombination der unterschiedlichen Engine-Stärken – kein Einzel-Scanner bietet optimalen Schutz vor allen Gefahren
- Bestmögliche Minimierung des Infektionsrisikos
- Bedeutender Preis-Leistungsvorteil, da sogar günstiger als die meisten Produkte mit nur einer Antiviren-Engine

### VORTEILE

- **Unterstützt die branchenführenden Messaging-Plattformen Microsoft Exchange Server 2000, 2003, 2007 und Lotus Domino**
- **Unterstützt mehrere Antiviren-Engines für eine höhere Viren-Erkennungsrate und schnellere Gegenmaßnahmen**
- **Spürt dank des leistungsfähigen Trojan & Executable Scanner neue schädliche exe-Dateien OHNE zusätzliche Viren-Updates auf**
- **Deaktiviert E-Mail-Exploits und HTML-Skripten per Email Exploit Engine und HTML Sanitizer**



## Virenkontrolle mit mehreren Scan-Engines

GFI MailSecurity setzt zur Überprüfung eingehender E-Mails mehrere Viren-Scanner ein. Die Verwendung verschiedener Engines verkürzt die durchschnittliche Wartezeit bis zum Erhalt aktualisierter Signatur-Updates und verringert die Gefahr, mit einem neuen Virus infiziert zu werden. Es gibt keinen Antiviren-Hersteller, der stets am schnellsten auf akute Bedrohungen reagiert. Wird ein neuer Virus bekannt, hängt ein rasches Bereitstellen entsprechender Updates z. B. davon ab, wo der Schädling entdeckt wurde. Die Verwendung mehrerer Scan-Engines erhöht die Chance, dass mindestens eine von ihnen zeitnah aktualisiert wird und rechtzeitig Schutz bietet. Zudem wendet jede Lösung ihre eigene Heuristik an und besitzt individuelle Abwehrmethoden. Einige Scanner erkennen bestimmte Virenarten samt Untergruppen besser als andere, die wiederum ihre eigenen speziellen Stärken haben. Fakt ist: Je mehr Scan-Engines eingesetzt werden, desto umfassender ist der Schutz.

## Überprüfung auf Trojaner und ausführbare Dateien

Der GFI MailSecurity Trojan & Executable Scanner entdeckt unbekannte böswillige exe-Dateien (z. B. Trojaner), indem er überprüft, welche Auswirkungen das Starten einer ausführbaren Datei hat. Trojaner können unbemerkt auf den Rechner eines Benutzers gelangen und einem Angreifer uneingeschränkten Zugriff auf die Daten des Computers ermöglichen. Noch unbekannte Trojaner werden von herkömmlicher Antiviren-Software NICHT identifiziert, da deren Überprüfungen nur auf Signaturen basieren. Der Trojan & Executable Scanner hingegen setzt zuverlässige und intelligente Scan-Methoden ein, die den Gefährdungsgrad einer exe-Datei bestimmen. Die Datei wird disassembliert, die Überprüfung ihrer Prozessabläufe findet in Echtzeit statt, und vorgegebene Aktionen werden mit einer Datenbank bekannter böswilliger Aktionen verglichen. Danach stellt der Scanner sämtliche exe-Dateien unter Quarantäne, von denen verdächtige Aktionen ausgehen, z. B. das Aufnehmen einer Modem- oder Netzwerk-Verbindung oder der Zugriff auf Adressbücher.

## Norman Virus Control & BitDefender – bereits im Lieferumfang enthalten

GFI MailSecurity wird mit den Scan-Engines Norman Virus Control und BitDefender ausgeliefert. Norman Virus Control ist als professionelle Antiviren-Engine bereits 32 Mal mit dem "Virus Bulletin 100% Award" ausgezeichnet worden. Zudem hat das Produkt die ICSCA- und Checkmark-Zertifizierung erhalten. BitDefender ist eine sehr schnelle, flexibel einsetzbare Antiviren-Engine und überzeugt durch die Anzahl der Formate, die erkannt und gescannt werden. BitDefender ist ebenfalls ICSCA-zertifiziert und wurde mit dem "Virus Bulletin 100% Award" und dem "European IT Prize 2002" prämiert. GFI MailSecurity sucht automatisch nach neuen Virendefinitionen für Norman Virus Control und BitDefender und aktualisiert diese selbstständig. Im Preis von GFI MailSecurity ist ein Update-Abonnement für 1 Jahr enthalten.

## Antiviren-Engines von Kaspersky, McAfee und AVG (optional)

Für noch mehr Sicherheit ist es möglich, die Antiviren-Engines von Kaspersky, McAfee und/oder AVG als zusätzliche Lösungen zur Virenabwehr oder als Ersatz für eine der anderen Engines einzusetzen. Kaspersky Anti-Virus ist ICSCA-zertifiziert und überzeugt durch seine unübertroffene Scan-Tiefe. Die Engine wird auch wegen ihrer schnellen Bereitstellung aktualisierter Virensignaturen und der heuristischen Technologie, die unbekannte Viren effizient neutralisiert, geschätzt. Die Stärken der McAfee Antiviren-Engine liegen in der Identifizierung von Angriffen, die nicht direkt über Viren, sondern z. B. mit Hilfe von ActiveX-Steuer-elementen gestartet werden. AVG Technologies ist seit über 15 Jahren einer der weltweit führenden Anbieter von Lösungen zur Identifizierung, Analyse und Abwehr von Viren.

## Automatisches Entfernen von HTML-Skripten

Bei E-Mails im HTML-Format können Hacker und Viren-Programmierer Befehle einbinden, die beim Öffnen der Nachricht umgehend ausgelöst werden. GFI MailSecurity scannt nach Skript-Code im Textkörper der Mitteilung und deaktiviert alle Befehle, bevor die gesäuberte HTML-E-Mail an den Empfänger weitergeleitet wird. GFI MailSecurity ist das einzige Produkt, das mit Hilfe einer von GFI patentierten Technologie vor potenziell gefährlichen HTML-Mails schützt.



Konfigurationskonsole von GFI MailSecurity



Konfiguration der Anhangskontrolle

## Systemanforderungen

- Microsoft Windows Server 2003 Standard/Enterprise (x86 Edition), Windows Server 2008 (x86 Edition), Windows 2000 Professional/Server/Advanced Server (mit SP1 oder höher) oder Windows XP
- Hinweis: Da die im Lieferumfang von Microsoft Windows XP enthaltene Version der Internet Information Services (IIS) nur 10 gleichzeitige Client-Verbindungen unterstützt, sind bei der Installation von GFI MailSecurity auf einem Rechner mit diesem Microsoft-Betriebssystem Leistungseinbußen möglich.
- Unterstützung von optionalem Microsoft Small Business Server (SBS) 2003/2008

↓ Weitere Informationen und eine kostenfreie Testversion stehen zum Abruf bereit auf <http://www.gfisoftware.de/de/mailsecurity/>

### Kontakt

#### Malta

Tel +356 2205 2000  
Fax +356 2138 2419  
sales@gfi.com

#### GB

Tel +44 (0)870 770 5370  
Fax +44 (0)870 770 5377  
sales@gfi.co.uk

#### USA

Tel +1 (888) 243-4329  
Fax +1 (919) 379-3402  
ussales@gfi.com

#### Asien/Pazifikraum/Südastralien

Tel +61 8 8273 3000  
Fax +61 8 8273 3099  
sales@gfiap.com

Weitere Niederlassungen von GFI: <http://www.gfisoftware.de/de/company/contact.htm>

**Microsoft**  
GOLD CERTIFIED

Partner

**GFI**