

# GFI EventsManager

Überwachung, Verwaltung und Archivierung von Netzwerkereignissen

■ Tausende von Kundeninstallationen

## Überwachung, Verwaltung und Archivierung von Ereignissen leicht gemacht

Systemereignisse, die regelmäßig in sehr großer Zahl im Netzwerk anfallen, bieten Organisationen wertvolle Informationen zur Einhaltung immer strengerer rechtlicher Überwachungsvorgaben und branchenspezifischer Compliance-Anforderungen. Die Ereignisüberwachung ermöglicht es außerdem, rascher auf Gefahren für die IT-Sicherheit reagieren zu können. Aufgrund von wachsenden Bedrohungen für die betriebliche Kontinuität ist das Monitoring von IT-Umgebungen in Echtzeit wichtiger denn je – ebenso wie die Möglichkeit, anfallende Daten für aussagekräftige Berichte aufzubereiten und zu analysieren, um daraus gesetzeskonforme Maßnahmen abzuleiten.

Ohne Unterstützung durch spezielle Tools ist es jedoch nicht möglich, relevante Informationen aus tausenden von Ereigniseneffizient zu erfassen. GFI EventsManager erleichtert Systemadministratoren die Überwachung, Verwaltung und Archivierung von Sicherheitsereignissen im Netzwerk – kostengünstig und effizient.

Unternehmen können dank GFI EventsManager gesetzliche und branchenspezifische Compliance-Vorgaben wie SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standard) und HIPAA (Health Insurance Portability and Accountability Act) leichter einhalten. Die preisgekrönte Sicherheitslösung unterstützt die Verarbeitung von Ereignissen unterschiedlichster Art, ob W3C- und Windows-Ereignisse oder Syslog-Meldungen und SNMP-Traps von Geräten wie Firewalls, Router, Sensoren und unternehmensspezifische Lösungen.

Durch die Unterstützung von Hardware der 20 weltweit größten Hersteller und von individuellen Geräten lässt sich eine breite Anzahl an Produkten kontrollieren. Kritische Ereignisse zu Systemzustand und Betriebsstatus jedes einzelnen Geräts werden umgehend gemeldet und Daten zur weitergehenden Analyse erfasst.

### VORTEILE

- Ermöglicht die zentrale Erfassung von Syslog-, W3C- und Windows-Ereignissen sowie der SNMP-Traps von Firewalls, Servern, Routern, Switches, Telefonanlagen, PCs u. v. m.
- Steigert die Netzwerk-Uptime und erlaubt eine rasche Problemerkennung durch Echtzeit-Warnungen
- Fördert eine effiziente, kostensparende Überwachung und Verwaltung des gesamten Netzwerks
- Bietet SQL-Server-Auditing für Microsoft SQL Server 2000, 2005 und 2008 sowie MSDE und Microsoft SQL Server Express



## Echtzeit-Warnungen per SNMPv2-Traps

Bei kritischen Ereignissen im Netzwerk werden Gegenmaßnahmen eingeleitet, wie das Starten von Skripten zur Behebung oder die Alarmierung von Mitarbeitern per E-Mail, Netzwerknachricht oder SMS (per E-Mail-zu-SMS-Gateway/Dienst). Erweiterte Warnmöglichkeiten bestehen durch die neue Unterstützung von SNMPv2-Traps. SNMP-Meldungen erlauben die Integration von GFI EventsManager mit zuvor bereits vorhandenen oder allgemeinen Überwachungslösungen.

## Installation und Nutzerfreundlichkeit

GFI EventsManager 8.1 lässt sich leichter installieren und verwalten. Neben verschiedenen Leistungssteigerungen hilft eine optimierte Dokumentation beim schnelleren Installieren des Produkts. Dank neuer Leitfäden zum Schnelleinstieg lassen sich Ereignisquellen rascher hinzuzufügen, Regeln schneller erstellen und Datenbankaufgaben effizienter erledigen. Auch das zugehörige ReportPack-Berichtmodul ist einfacher abrufbar und einzurichten. Es bietet zudem auf den PCI-Sicherheitsstandard(PaymentCardIndustry) zugeschnittene Reports.

## Berichte zu wichtigen Sicherheitsereignissen im Netzwerk

Das kostenfreie ReportPack-Berichtmodul ermöglicht die Erstellung neuer Reports oder die Anpassung bereits vorhandener Standardberichte für die Bereiche:

- Payment Card Industry (PCI)
- Kontoverwendung
- Kontoverwaltung
- Richtlinienänderungen
- Objektzugriffe
- Anwendungs-Management
- Drucker-Server
- Windows-Ereignisprotokoll
- Ereignistrends

## Zentralisierte Ereignisprotokollierung

Ereignisprotokolle werden automatisch erstellt und erweitert, ob von Hintergrundprozessen oder durch Anwenderaktionen. Die Speicherung der Dateien erfolgt jedoch oft an verschiedenen Orten. GFI EventsManager sichert alle erfassten Ereignisprotokolle in einer SQL-Datenbank, ob lokal oder entfernt. Backups der Protokolle nach einem festgelegten Zeitplan sind ebenfalls möglich.

## Analyse von Ereignisprotokollen (SNMP-Traps, Windows-Ereignisprotokolle, W3C-Protokolle und Syslog)

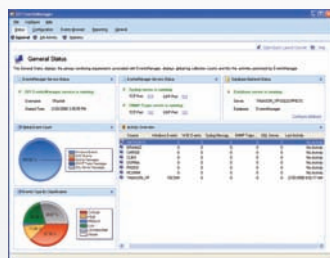
Aufgabe von Netzwerkadministratoren ist es unter anderem, mit zahlreichen kryptischen Einträgen überfüllte Sicherheitsprotokolle zu analysieren. GFI EventsManager hilft ihnen beim netzwerkweiten Kontrollieren und Verwalten von Event-Logs, um relevante Ereignisse aus Windows-Ereignisprotokollen, W3C-Protokollen oder Syslog-Meldungen unterschiedlichster Netzwerkquellen herauszufiltern. Die Unterstützung von SNMP Version 3 (Simple Network Management Protocol) ermöglicht die Überwachung und Meldung von Zustand und Betriebsstatus unterschiedlichster Netzwerkelemente wie Router, Sensoren und Firewalls.

## "Certified for Windows Server® 2008" und Unterstützung von Microsoft Windows Vista

GFI EventsManager ist offiziell für Microsoft Windows Server 2008 zertifiziert und jetzt auch unter Microsoft Windows Vista lauffähig. Das neue Protokollformat beider Plattformen wird ebenfalls erfasst und gemeinsam mit anderen Formaten einheitlich dargestellt, um Systemverantwortlichen einen einfacheren Gesamtüberblick über alle Systeme hinweg zu bieten. Weiterhin unterstützt werden Microsoft Windows 2000, XP und 2003.

## Granulare Ereigniskontrolle

GFI EventsManager unterstützt die Überwachung einer großen Auswahl an Plattformen und Hardware. Unterschiedliche Protokolltypen mit Windows-Ereignissen, Syslog-Meldungen, W3C-Events und SNMP-Traps von Netzwerkelementen werden zentral gesichert und analysiert. Administratoren ist es möglich, relevante Daten von Windows-Computern und Drittgeräten mit einer hohen Granularität zu erfassen und Informationen auch auf Ebene erweiterter Tags zu verarbeiten. Über die weitergehende Bearbeitung kann dann umgehend auf Grundlage der vorliegenden Ergebnisse entschieden werden – ohne zusätzliche Datenverwaltung.



Verwaltungskonsolle



Erste-Schritte-Dialog

## Systemanforderungen

- Systemanforderungen – GFI EventsManager-Computer:** Microsoft .NET Framework 2.0, Microsoft Windows 2000, XP, Server 2003/2008, Unterstützung von optionalem Microsoft Small Business Server (SBS) 2003 und 2008, Microsoft Data Access Components (MDAC) 2.8 oder später, Microsoft Access, MSDE oder Microsoft SQL Express (kostenfrei; automatischer Download bei Installation) oder Microsoft SQL Server 2000/2005/2008
- Software-Anforderungen – zu überprüfende Computer:** Zur Kontrolle der Windows-Ereignisprotokolle: aktivierter Remoteregistrierungsdienst, aktivierte Windows-Sicherheitsüberwachung, überwachte Windows-Vista-Rechner in derselben Domäne wie GFI EventsManager-Computer befindlich und Vista-Benutzerkontosteuuerung (User Account Control, UAC) deaktiviert; zur Kontrolle der W3C-Protokolle: Quellverzeichnisse müssen über Windows-Freigaben zugänglich sein
- Syslog und SNMP-Traps:** Konfigurierung von Quellen/Absendern für den Meldungsversand an Computer/IP-Adresse mit GFI EventsManager

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

**Microsoft**  
GOLD CERTIFIED

Partner

### 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>

**GFI**