

---

## **De noodzaak tot effectief eventbeheer**

---

Uitdagingen, strategieën en oplossingen voor effectief eventbeheer

GFI EventsManager is gebaseerd op het feit dat beheer van event logs essentieel is maar vaak over het hoofd wordt gezien. Logs en het beheer daarvan zijn echter uiterst belangrijke onderdelen van het beheer van computersystemen. Dit white paper laat zien welke rol GFI EventsManager kan spelen en hoe het product een waardevolle bijdrage kan leveren.

---

## Inleiding

Onderschat, ondergewaardeerd en onderbenut: eventbeheer wordt vaak beschouwd als een vervelende en ondankbare taak. Systeembeheerders blijven uit de buurt van event logs en de events daarin vanwege tijdgebrek en een gebrek aan duidelijke definities. Events vormen echter belangrijke informatiebronnen die in vele bedrijfsprocessen kunnen worden benut, zoals het zoeken naar informatie en het nemen van beslissingen. Daarnaast zijn er diverse wetten die gebieden dat logs onderhouden en bewaard moeten worden. Dit white paper bespreekt hoe GFI EventsManager bedrijven kan helpen belangrijke doelen te bereiken.

Inleiding .....	2
Eventbeheer en GFI EventsManager.....	2
Naleving van wetgeving en voorschriften.....	5
Beveiliging van informatiesystemen .....	6
Monitoring van systeemprestaties.....	7
Forensische onderzoeken .....	8
GFI EventsManager ROI en voordelen.....	9
Conclusie.....	9
Over GFI.....	11

---

## Eventbeheer en GFI EventsManager

### Wat zijn events?

Events zijn records die worden gegenereerd en in specifieke locaties worden opgeslagen door processen in een computersysteem. Events worden getriggerd door gebruikers of door een automatische procedure. Er zijn vele voorbeelden van events:

- De installatie van nieuwe software genereert een groot aantal verschillende events (in Windows Event Logs) met betrekking tot de installatieprocedures en bestandsgegevens.
- Webserver loggen grote aantallen events (in W3C event logs) met betrekking tot de gebruikers die van de diensten erop gebruikmaken.
- Firewalls en network routers loggen automatisch events (Syslogs) met betrekking tot toegestane, geweigerde en ongeautoriseerde toegang.

Gelogde events worden automatisch opgeslagen in tekstbestanden zoals W3C logs (vooral gebruikt in webserver) of binaire bestanden zoals Windows Event Logs. Deze kunnen ook over het netwerk via TCP/IP naar een logserver worden verstuurd voor opslag (bijvoorbeeld Syslogs die op Unix/Linuxmachines worden gebruikt. De logserver slaat de ontvangen event logs op in een bestand of database. Eventbeheer is het proces van beheer, analyse en rapportage dat dat hoort bij het beheer van eventgegevens die zijn gegenereerd door computers en gebruikers en

de logs waarin de gegenereerde events zijn opgeslagen.

### **Problemen met eventbeheer**

De ontevredenheid rondom eventbeheer vindt haar oorsprong in het feit dat fabrikanten van besturingssystemen en apparatuur meestal tools voor eventbeheer leveren met zeer beperkte functionaliteit.

Bovendien zijn eventgegevens meestal:

- Volumineus – op een typisch middelgroot netwerk worden elke dag honderdduizenden events gegenereerd die allemaal worden gelogd.
- Vaag – de eventgegevens in logbestanden zijn meestal erg cryptisch.
- Verspreid – eventgegevens worden opgeslagen op verschillende locaties (computers, servers en andere apparatuur) op het netwerk.

Ook zijn er problemen bij het beheer van eventgegevens met behulp van de standaard geleverde tools waarbij:

- beheerders niet op de hoogte kunnen worden gebracht wanneer bepaalde problematische events worden gelogd.
- de zoek- en filtercapaciteiten te beperkt zijn.

Deze zaken leiden tot problemen met betrekking tot mankracht en geld. Efficiënte monitoring van events vereist planning van extra tijd, geld en het aantrekken van de benodigde expertise. Dit dwingt bedrijven vaak af te wijken van 'best practice'-principes en ofwel de gemakkelijkste benadering te kiezen of events helemaal niet te monitoren.

### **De wedergeboorte van eventbeheer**

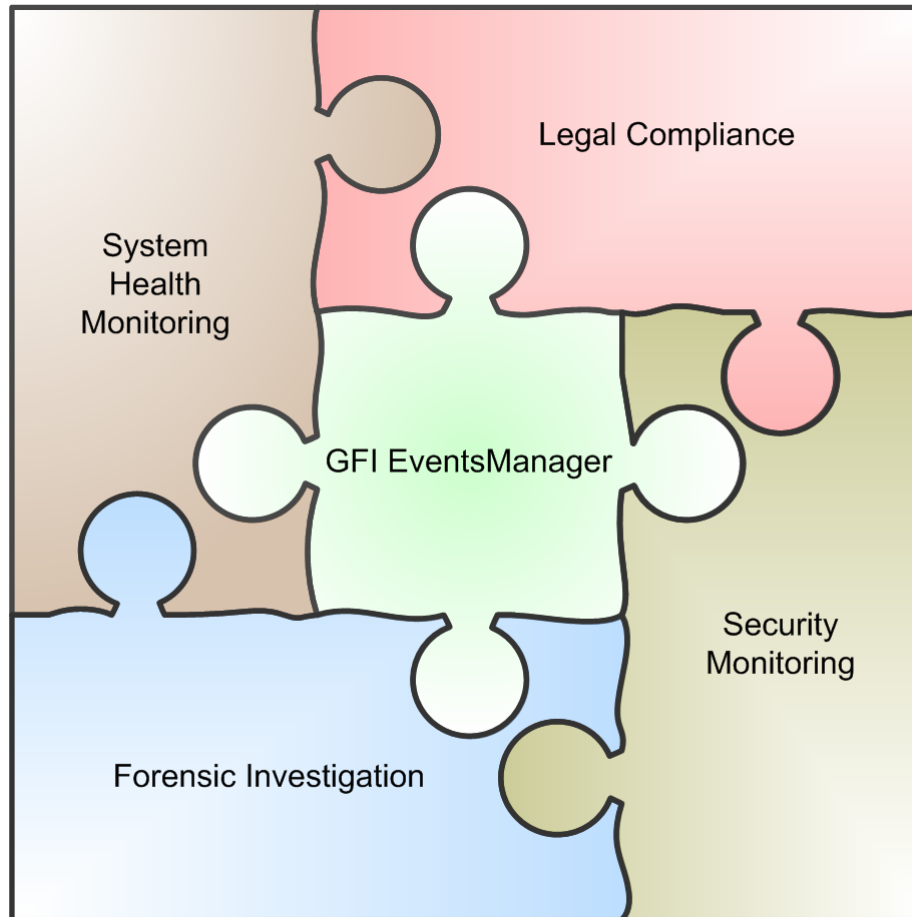
De introductie van wetgeving als S-OX, HIPAA, GLBA, PATRIOT Act en FISMA heeft grote gevolgen gehad voor de houding ten opzichte van eventbeheer. Bedrijven zijn nu wettelijk verplicht om log- en eventgegevens te onderhouden en regelmatig te controleren. De meer ervaren IT-managers realiseren zich steeds beter dat eventgegevens essentiële en zeer waardevolle tools zijn bij de forensische analyse van systeemfouten in inbraken. Systeembeheerders komen erachter dat proactieve controle van events een waarschuwingssysteem vormt voor diverse soorten fouten en dus de kans biedt om actie te ondernemen voordat er schade kan ontstaan.

GFI EventsManager automatiseert en vereenvoudigt de taken die nodig zijn voor eventbeheer en maakt er een eenvoudig, functioneel proces van. Het is een tool die:

- De verzameling van events uit logbestanden op verschillende locaties automatiseert.
- Irrelevante informatie verwijdert zonder dat belangrijke gegevens verloren gaan.

- Eén enkele gebruikersinterface biedt voor de belangrijkste soorten events zodat het relatief eenvoudig is om door events te bladeren.
- Uitleg geeft bij gelogde events.
- Onderzoek van specifieke problemen mogelijk maakt met uitgebreide query tools.
- Uitgebreide analyserapporten biedt die managers en controleurs helpen bij het identificeren van veranderingen en dus bij het nemen van beslissingen.

### Gebruik van eventbeheer



Met GFI EventsManager kunnen events voor diverse overlappende doeleinden worden gebruikt, waaronder:

- Naleving van wetgeving en reguleringen
- Beveiliging van informatiesystemen
- Monitoring van systeemprestaties
- Forensisch onderzoek

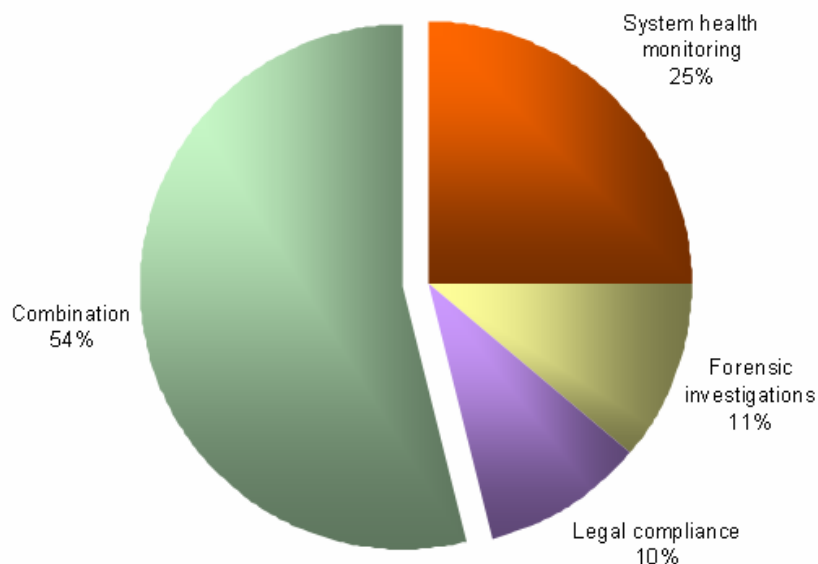
## Naleving van wetgeving en voorschriften

Een belangrijk doel van het monitoren van events is naleving van wetgeving en voorschriften. Bedrijven zijn verplicht om hun controlesystemen regelmatig te evalueren. Om aan deze eisen te voldoen moet men eventgegevens in logs beschouwen als de primaire bron voor het verkrijgen van informatie, het bepalen van de mate waarin aan eisen wordt voldaan en het identificeren van gebreken.

### Behoud van logs

Uit de peiling van SANS over firewall logs in 2005 is gebleken dat:

- 28% de logs langer dan een jaar bewaart
- 14% de logs een maand of korter bewaart
- 31% de logs minder dan 3 maanden bewaart
- 14% bewaart logs totdat de schijf vol is
- 13% geen logs bewaart



Bovendien blijkt uit de enquête van SANS uit 2006 over het gebruik van logs dat:

- 25% logs gebruikt voor het monitoren van systeemprestaties
- 11% logs uitsluitend voor forensisch onderzoek gebruikt
- 10% logs uitsluitend gebruikt om te voldoen aan wettelijke eisen
- 54% logs gebruikt voor een combinatie van bovenstaande factoren

Het bijhouden van beveiligde, knoeibestendige archieven van de originele, ongewijzigde events in de logbestanden is essentieel als u wilt bewijzen dat u aan wettelijke eisen voldoet.

Afhankelijk van de betreffende wet en de staat moeten event logs in de Verenigde Staten

worden bewaard voor een periode die varieert van zes maanden tot zeven jaar. Dit betekent dat een belangrijk deel van de respondenten in de enquête van SANS uit 2006 niet aan wettelijke eisen voldoet.

### **Controle van logs**

Om aan wettelijke eisen te voldoen moeten organisaties tevens aantonen dat ze de toegang tot systeembronnen goed controleren. Instanties zoals NIST raden aan om minstens twee keer per week de eventgegevens te controleren.

Concurrenten van GFI EventsManager op de MKB-markt bieden geen duidelijke strategie voor het bewaren van events om aan wetten en voorschriften te voldoen. Dit is een functionaliteit die alleen wordt benadrukt door concurrenten die zich op grote bedrijven richten. En hoewel de concurrenten van GFI EventsManager op de MKB-markt allemaal beweren te helpen bij het voldoen aan wettelijke eisen, staan sommigen de verwijdering van database archieven toe terwijl anderen niet alle events verzamelen. Dit betekent een serieuze ondermijning van pogingen om aan wettelijke eisen te voldoen.

Met GFI EventsManager kunnen organisaties events met betrekking tot logins, accountbeheer, toegangscontrole en meer verzamelen, opslaan en erover rapporteren. Databases kunnen ook worden gearchiveerd voor back-ups van alle geproduceerde rapporten. GFI EventsManager brengt geen wijzigingen aan in de originele logbestanden of de eventgegevens die zich daarin bevinden en zorgt er dus voor dat er wordt voldaan aan wetten die eisen dat originele logbestanden worden bewaard.

---

## **Beveiliging van informatiesystemen**

Nu bijna alle bedrijven afhankelijk zijn van informatiesystemen, is de beveiliging van informatiesystemen een zeer belangrijk aspect van het monitoren van events. Beveiligingsproblemen leiden tot verlies van omzet, verlies van klanten en een verslechterde reputatie. Het kost veel tijd en geld om hiervan te herstellen.

Dit aspect van monitoring van events overlapt met het voldoen aan wettelijke eisen. Er zijn bepaalde informatiesysteemstandaarden (bijvoorbeeld COBIT 4.0, ISO 17799) waaraan voldaan moet worden. Al deze standaarden leggen de nadruk op de implementatie van eventmonitoring als één van de belangrijkste methoden van informatiesysteembeveiliging.

Met GFI EventsManager weet u dat uw beveiliging in orde is. GFI EventsManager biedt systeembeheerders de volgende functionaliteiten:

- 24/7 Realtime inbraakdetectie en alerts.
- Tijdige waarschuwingen zodat beheerders inbraken tegen kunnen gaan.
- Een backupfaciliteit die voorkomt dat logdata verwijderd worden.
- Intelligente en configureerbare regels voor eventverwerking die ook aanvallen van binnenuit

detecteren.

- Configureerbare waarschuwingfuncties waarmee de waarschuwingsmethodes kunnen worden aangepast naargelang het tijdstip.

GFI EventsManager biedt tevens uitgebreide analyse- en rapportagefunctionaliteiten. Dit betekent dat er regelmatig rapporten kunnen worden uitgebracht over bijvoorbeeld wijzigingen in privileges van bepaalde gebruikers. Ook heeft u zicht op geslaagde en mislukte inlogpogingen en pogingen om toegang te krijgen tot bestanden en mappen die niet voor iedereen toegankelijk zijn.

Detectie van ongebruikelijk gedrag is cruciaal voor het detecteren van misbruik van systemen en hulpbronnen door gebruikers met en zonder privileges. Als u beveiligingsbeleid implementeert en gebruikers monitort, kunt u ongebruikelijk gedrag detecteren zonder dat de bedrijfsvoering in gevaar komt.

### **Maatstaven voor prestaties van werknemers**

Het is mogelijk om het systeemgebruik van werknemers te meten aan de hand van configureerbare regels en regelsets. Moderne toegangssystemen met en zonder pasjes en PABX- en VOIP-systemen zijn allemaal geïntegreerd om op het bedrijfsnetwerk te kunnen functioneren en genereren logs die in combinatie met GFI EventsManager kunnen worden gebruikt.

Monitoring van toegang en van telefoniesystemen in combinatie met eventmonitoring geeft bedrijven de kans om hun werknemers continu te monitoren en te zien wanneer ze op kantoor arriveren, wanneer ze persoonlijke telefoongesprekken voeren, wat ze doen en welke bestanden ze tijdens hun werkdag openen. Dit kan allemaal met behulp van slechts één console. Het product is dus niet alleen een beveiligingstool maar is ook handig voor de afdeling personeelszaken: het is mogelijk om voor iedere werknemer een rapport te creëren dat onder andere voor beoordelingen kan worden gebruikt.

---

### **Monitoring van systeemprestaties**

Het is essentieel om downtime tot een minimum terug te brengen om verlies van klanten, reputatie en inkomsten te voorkomen. Bij het herstellen van een systeem gaat meestal 90% van de tijd op aan handmatig onderzoek naar de oorzaak van de systeemfouten. In sommige gevallen is een volledig herstel niet eens mogelijk. Dit betekent onherroepelijk verlies van bedrijfsgegevens, belangrijke documenten of broncode.

Eventmanagement helpt events te identificeren die symptomen van potentiële hardwarefouten zijn. Error events worden wanneer zich I/O-fouten voordoen op harde schijven. Daarnaast komen error events voor wanneer applicaties niet werken vanwege problemen met geheugenmodules. Dit zijn slechts twee voorbeelden van mogelijke problemen.

Eventmanagement stelt systeembeheerders in staat om proactief te zijn en systeemcomponenten te repareren of te vervangen voordat er problemen ontstaan. Het systeem wordt zo een stuk betrouwbaarder. Hoewel de voordelen van een betrouwbaar systeem misschien niet meteen zichtbaar zijn, zijn de nadelen van downtime onmiddellijk merkbaar.

Typische eventpatronen helpen ook bij het opsporen van toekomstige risico's zodat de systeembeheerder preventief onderhoud kan uitvoeren. Dergelijke patronen kunnen een systeembeheerder bijvoorbeeld helpen zich te realiseren dat de opslagruimte op harde schijf na elke drie maanden bijna vol is. De beheerder kan preventieve maatregelen nemen door backup- en onderhoudstaken te plannen zodat de volledige capaciteit niet bereikt wordt.

GFI EventsManager biedt realtime monitoring van kritieke applicaties en IT-systemen. De door GFI EventsManager gebruikte regelset voor systeemprestaties is een belangrijke tool die de systeembeheerder in staat stelt om altijd controle te hebben over wat er op het netwerk gebeurt. Systeembeheerders kunnen de huidige staat van het netwerk monitoren met de scanningmonitor en worden gewaarschuwd wanneer er belangrijke systeemgerelateerde events plaatsvinden. Dankzij configureerbare alerts kan de beheerder zelfs worden gewaarschuwd wanneer hij of zij niet op kantoor is (via e-mail of sms).

---

## Forensische onderzoeken

Naast het voldoen aan wettelijke voorschriften en het beveiligen van informatiesystemen dient GFI EventsManager nog een belangrijk doel. In de SANS-enquête uit 2006 gaf een belangrijk deel van de ondervraagde bedrijven aan dat ze systemen voor logmanagement gebruikten voor forensisch onderzoek naar dubieuze events op het netwerk.

In ieder forensisch onderzoek is bewijs uit zoveel mogelijk verschillende bronnen noodzakelijk. Op die manier krijgt u onweerlegbaar bewijs van de feiten. Logs en de eventgegevens hierin zijn van onschatbare waarde bij het reconstrueren van de chronologie van events die op een systeem hebben plaatsgevonden. Eventgegevens kunnen dus belangrijk bewijsmateriaal vormen bij rechtszaken. Bovendien is het heel belangrijk dat het proces van forensisch onderzoek zo snel en gestroomlijnd mogelijk is zodat aan strikte deadlines wordt voldaan.

Forensisch onderzoek is een belangrijk aspect van eventbeheer dat door alle fabrikanten van software voor eventbeheer in de MKB-markt wordt benadrukt. Softwareproducten met functionaliteiten voor forensische analyse worden vaak gezien als eenvoudige, goedkope alternatieven voor gespecialiseerde beveiligingsadviseurs en externe audits.

Als u overweegt om software voor forensische analyse aan te schaffen, dient u met diverse factoren rekening te houden, namelijk:

- De identificatie van (kwaadwillende of onbedoelde) toegang op meervoudige en diverse platforms.

- Veilige opslag en onderhoud van back-ups van logs zodat er niet mee geknoeid kan worden door hackers en andere kwaadwillenden.
- De diverse filter- en bladertools die u nodig heeft voor forensische onderzoeken.
- Het tijdsbestek waarin zoekopdrachten worden uitgevoerd en rapporten worden gegenereerd.

GFI EventsManager blinkt uit in analyse van forensische data dankzij het uitgebreide scala aan zoek- en rapportagemogelijkheden. Deze twee kenmerken en de onderliggende technologie van GFI Events Manager geven het product een zeer goede positie in de markt.

---

## **GFI EventsManager ROI en voordelen**

“Op incidenten reageren kost meer dan proactief zijn!” (Abe Usher, Security Expert, Sharp Ideas). De voordelen van GFI EventsManager op het gebied van ROI (Return on Investment) zijn cruciaal bij het helpen van bedrijven in het geval van problemen op het gebied van netwerkbeveiliging, het voldoen aan wettelijke eisen en systeemprestaties (problemen waarvoor geen enkel bedrijf immuun is). Het product functioneert als een proactieve verzekeringspolis die niet alleen bedrijven beschermt bij pijnlijke incidenten maar zelfs voorkomt dat dergelijke incidenten plaatsvinden. Dit beschermt bedrijven tegen verlies van geld vanwege verloren werkuren, verlies van klanten, verlies van verkoop en reputatieverlies.

GFI EventsManager kan tevens forensische analyses uitvoeren op dubieuze events die zijn veroorzaakt door mensen die al bij het bedrijf werken. U kunt dus forensische onderzoeken uitvoeren zonder dat u daarvoor dure bureaus hoeft in te huren. U heeft dus geen pottenkijkers en u bespaart bovendien geld.

Een ander voordeel van GFI EventsManager is de mogelijkheid om de prestaties van werknemers te meten. Met GFI EventsManager kunnen bedrijven het gedrag van hun werknemers monitoren met het oog op beoordelingen. Dit neemt een hoop ambiguïteit weg in een normaliter grijs onderdeel van beoordelingsprocedures, en dat met slechts één console. Het product helpt bedrijven hun geld en andere middelen te investeren waar ze het meest nodig zijn.

---

## **Conclusie**

Met GFI EventsManager kunnen bedrijven belangrijke doelen bereiken die zeer belangrijk zijn voor het welzijn van het bedrijf op het gebied van het voldoen aan wettelijke eisen, beveiliging van informatiesystemen, systeemprestaties en forensisch onderzoek. Deze doelen worden bereikt door het gebruik van technologie die eenvoudig in het gebruik is en waarvoor geen uitgebreide training of technische ondersteuning nodig is. Dankzij de praktische benadering van de software kunnen bedrijven er zeker van zijn dat ze niet alleen waar voor hun geld krijgen maar ook ‘best practice’-principes aanwenden die zowel op korte als lange termijn hun

vruchten afwerpen.

---

## Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

