

GFI White Paper

The need for effective event management

Challenges, strategies and solutions to effective event
management

GFI EventsManager™ is based on the simple fact that event log management is an indispensable tool in a corporate environment; a concept that, due to its simplicity, system administrators often tend to overlook. Logs and their management are, however, one of the most important aspects in computer systems management.

This white paper shows where GFI EventsManager fits in this picture and how it is a valuable asset in the corporate toolbox.

Contents

Introduction.....	3
Events management and GFI EventsManager.....	3
Legal compliance.....	5
Information system security.....	6
System health monitoring.....	7
Forensic investigations.....	7
GFI EventsManager ROI and benefits.....	8
Conclusion.....	8
About GFI®.....	8

Introduction

Underrated, undervalued and underutilized – events management is most often rated as a tedious and ungrateful task. System administrators shy away from event logs and the events contained within, citing lack of time and clear definitions to the events produced as the principle detractors to the events management process. Events however constitute an invaluable source of information that can be utilized in a number of business processes such as fact finding and decision making. Various laws also mandate that logs have to be maintained and reviewed. This paper examines various corporate needs and provides information on how GFI EventsManager can help corporations achieve important goals.

Events management and GFI EventsManager

What are events?

Events are records generated and stored in specific locations by processes within a computer system. Events are triggered either by a user or by an automatic/background process. Examples of the events logged abound:

- » The installation of new software generates a wide range of events (in Windows Event Logs) detailing the installation procedure and the file details.
- » Web servers log huge volumes of events (in W3C event logs) related to the users that access services offered on them.
- » Firewalls and network routers automatically log events (Syslogs) related to allowed, denied and unauthorized access.

Events logged are automatically stored in text files such as W3C logs (typically used in web servers) or binary files such as Windows Event Logs. Alternatively these can be transmitted on the network via TCP/IP for storage (ex. Syslogs used in Unix/Linux machines) to a log server. The log server then stores the received event logs in either a file or a database. Events management is the management, analysis and reporting process involved in the management of computer and user-generated events data and the logs within which the generated events are stored.

The problems with events management

The aura of discontent that surrounds events management derives from the fact that operating system and equipment manufacturers usually supply event analysis tools with only the most basic of features.

In addition, events data is typically:

- » Voluminous – Hundreds of thousands of events are generated daily on a typical medium-sized network, and all of them are logged.
- » Vague – Events data contained within log files are, more often than not, cryptic.
- » Distributed – Events data within logs is stored in various locations (computers, servers and other equipment) all over the network.
- » Problems also exist in the management of events data using the default tools supplied where:
 - » Administrators have no way of being alerted when particular problematic events are logged.
 - » The events browsing and filtering tools supplied by software and hardware makers have very limited search and filter capacities.

These issues create manpower and budgeting problems for corporations. To enable efficient events monitoring and the related policies, corporations often have to plan for extra time, resources and the acquisition of the required expertise. This often forces corporations to deviate from best practice principles and adopt the least-effort possible approach to log and events monitoring in general or, worse still, not to monitor events at all.

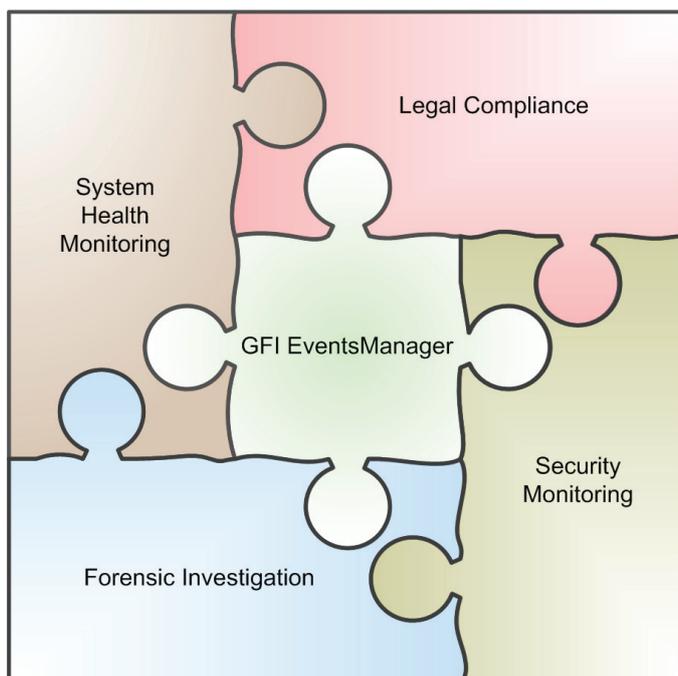
The renaissance of events management

The introduction of legislation such as S-OX, HIPAA, GLBA, PATRIOT Act and FISMA, has had a profound impact in the attitude to events management. Corporations are nowadays legally bound to maintain and proactively review log and events data in a continuing, self-assessment process. Increasingly, more experienced IT Management and audit staff are realizing that events data are an essential and invaluable tool in the forensic examination of systems failures and security breaches. Systems administrators are learning that the proactive review of events data serves as an early warning system for various types of failures and therefore allows them to take pre-emptive action before the actual damage occurs.

GFI EventsManager automates and simplifies the tasks involved in events management, transforming it into a do-able functional process. It is the tool that:

- » Automates events collection from various log file locations
- » Removes irrelevant noise (background process generated data) through the use of intelligent events processing while retaining all the important events data
- » Provides a single user interface for the major types of events, making events browsing a relatively simple task
- » Explains logged events using user-friendly explanations
- » Enables research of specific issues through extensive query tools
- » Provides extensive forensic and security analysis reports that aid auditors and management in identifying shifts in network resource trends and therefore help them in their decision making processes.

The uses of events management



Through GFI EventsManager, events can now actually be used for a number of intersecting purposes, among which are:

- » Legal compliance
- » Information systems security
- » System health monitoring
- » Forensic investigation.

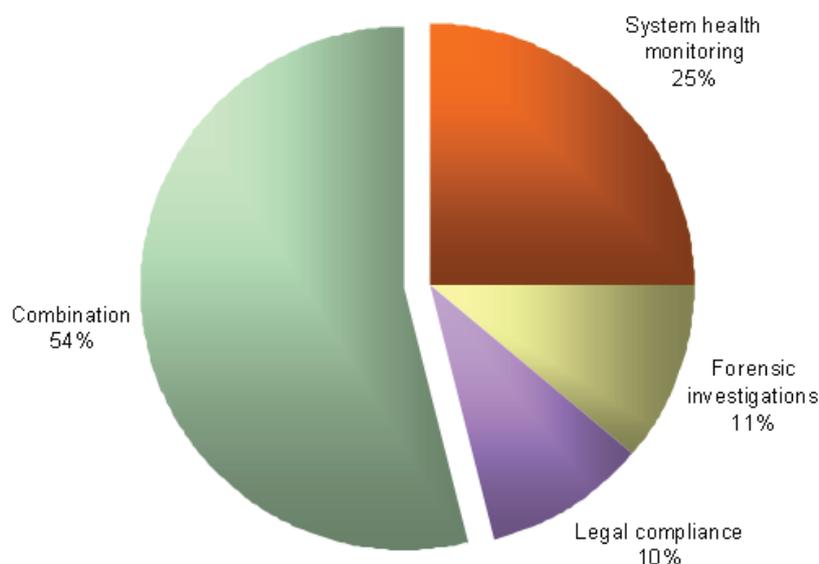
Legal compliance

One of the main purposes of events monitoring is legal compliance. Current laws and regulations oblige corporations to assess their internal control architecture on a regular basis. In order to comply with these laws, IT management staff and auditors have to consider events data contained within logs as the primary source through which to gain information, determine level of compliance and identify deficiencies.

Log retention

Respondents to the SANS 2005 poll on firewall logs report that:

- » 28% retain logs for over a year
- » 14% keep logs for a month or less
- » 31% keep logs for under 3 months
- » 14% maintain logs until the disk is full
- » 13% do not keep logs.



Furthermore a 2007 survey on log management by the SANS institute on the use of logs finds that:

- » 62% use logs to assess IT incidents and minimize downtime.
- » 46% use logs for automatic detection and analysis of security and performance incidents.
- » 44% use logs for IT controls and reporting to prevent system misuse, forensics.
- » 42% use logs for compliance and to prove compliance.

The retention of secure, tamper-proof archives of the original, unaltered events stored in log files is critical in proving evidence of legal compliance. Different laws demand that different event logs are maintained for dates that range from six months to seven years according to the law in question and the state where they were enacted. This effectively means that a substantial segment of the respondents to the 2006 SANS Firewall Log Monitoring survey may be in breach of one law or another.

Log review

To maintain legal compliance, organizations also need to provide physical documentation showing that they have appropriate control over access to resources. Guidelines issued by bodies such as NIST recommend an events data review at least twice a week.

Many event management solutions on the SME market do not offer a clear strategy on original events retention for legal compliance, which tends to be emphasized far more by those catering for the enterprise market. In addition, care must be taken as while most solutions claim to assist in legal compliance efforts, some of them permit the deletion of database archives, while others do not collect all the events stored in different formats – both of which seriously undermine any corporation's legal compliance efforts.

Through GFI EventsManager, organizations can collect, store, and report on events related to user logins, account management, access control management and more. Databases can also be archived to provide backing evidence on all reports produced. GFI EventsManager does not tamper with the original log files or the events data contained within, in any way, ensuring that the legal provisions that require original log file data retention are met.

Information system security

With almost all corporations nowadays relying on Information Systems to carry out their daily operations, information system security is a very important aspect of events monitoring which cannot be taken lightly. Security incidents result in loss of operations leading to loss of business, loss of face and customers. Recovering from such incidents is very time-consuming and expensive.

This aspect of events monitoring intersects with the legal compliance aspect. Enacting legal compliance implies that various information system standards (Ex. COBIT 4.0, ISO 17799) have to be adhered to. These standards all stress on the implementation of events monitoring as one of the main information systems security methods.

GFI EventsManager provides events management functionality which helps in achieving peace of mind with regards to security. GFI EventsManager provides the following functionality to systems administrators:

- » 24/7 real-time intrusion detection and alerting
- » An early warning system that enables administrators to take intrusion countermeasures
- » A backup facility that thwarts whoever tries to cover their tracks by deleting log data
- » Intelligent and configurable event processing rules that also detect malicious insider attacks
- » Configurable alerting features that change administrator notification methods according to the time of day.

GFI EventsManager also provides comprehensive analysis and reporting features. This allows regular auditing and reporting to senior management of, for example, changes to individuals' privilege levels. Audits also include reviewing and validating successful and unsuccessful logons, as well as all attempts to access restricted files and directories.

Detecting anomalous behavior is crucial in detecting system and resource abuse both by privileged and non-privileged users. Implementing a security policy and monitoring users against it enables anomalous behavior to be detected without hindering business operations.

Employee performance metrics

As a subset of information system security, employee performance metrics can be used to measure employee resource use against configurable rules and rule sets. Modern day card and keyless access systems, PABX or VOIP systems are all integrated to operate over the corporate network and most of them generate a log that can be used with GFI EventsManager.

Together with the events monitoring tools, the monitoring of access and telephony systems gives corporations the unique opportunity to measure staff behavior from when they access the corporate premises, to when they make personal calls, to what they do and which files they access during their work day. This is achieved through the use of a single console. Apart from the security aspect of this tool, human resources management now have the unique opportunity to utilize one tool that provides them with employee related reports that can be used for performance appraisals and other cost-reduction exercises.

System health monitoring

Reducing system downtime to a minimum is critical to organizations, since it leads to customer attrition, and loss of brand reliability and revenue. It is generally agreed that when restoring a system from backup, 90% of the time is taken up with manual investigation to identify the cause of the system failure. In some cases, full system recovery may not even be possible, leading to the irretrievable loss of business data, important documents or source code.

Event management helps identifying those events which could be symptoms of potential hardware failure. Error events are generated when hard-drives which are about to fail experience I/O failures. Error events are also generated when defective memory modules cause applications to fail when accessing the damaged area. These are only two examples from the large number of system and network components which may fail.

Event management enables system administrators to be proactive and to take corrective action to repair or replace critical system components before they fail. System reliability is therefore greatly increased. Although the benefits of having a reliable system may not be immediately apparent as this equates to having normal operations, the adverse effects of system downtime are immediately evident.

Typical event patterns also help the system administrator spot future system or utilization risks, allowing him to implement preventive maintenance. Such patterns may help a system administrator realize, for example, that hard disk storage is approaching full capacity every three months. The administrator can take preventive measures by scheduling backup and housekeeping tasks to prevent storage from reaching full capacity.

GFI EventsManager provides real-time monitoring of critical applications and IT systems. The system health rule set used by GFI EventsManager is an important tool in the system administrator toolkit, allowing him to be in control at all times on all that is happening on the network. Systems administrators can monitor current network state through the scanning monitor and is alerted when predefined important system-related events occur. Configurable alerts allow the administrator to be notified even when off-site, through email or sms.

Forensic investigations

Apart from legal compliance and information systems security, GFI EventsManager fulfils another important need that corporations have. In the June 2006 SANS survey, a substantial amount of the corporations interviewed indicate that they use Log Management systems to perform forensic investigation of dubious network occurrences.

In any forensic investigation, one crucial need is for evidence derived from as many different sources as possible. This helps establishing unequivocal proof of facts. Logs and the events data contained within makes them invaluable in building a timeline of the events that occurred on any given system. In this light, events data can be a very important piece of evidence that supports lawsuits. In addition to all of this, it is very important that the whole forensic investigation process is as fast and streamlined as possible to ensure that strict deadlines in presenting the evidence gained are met.

The forensic analysis aspect of events management is a strong value-added feature that almost all of the events management software makers in the SME market accentuate in their marketing. Software products which claim forensic analysis features are likely to be seen as simple, low cost alternatives to specialized security consultancy and external audits fees.

There are a number of issues that need to be addressed when considering forensic investigation software. These are:

- » The identification of access (malicious or unintentional) on multiple and diverse platforms
- » The secure storage and maintenance of log backups so that they cannot be compromised by malicious hackers and insiders
- » The range of filtering and browsing tools required for forensic investigation
- » The timeliness of the searches and the reports generated.

GFI EventsManager excels in forensic data examination due to its wide range of search and drill down tools and its comprehensive range of fast reporting capabilities and customizable reports. These two features and the underlying technology that drives GFI Events Manager enable GFI's offering to position itself very well in the forensic analysis aspect of events management tools for the SME market.

GFI EventsManager ROI and benefits

"The cost of being proactive is less than the cost of reacting to an incident!" (Abe Usher, Security Expert, Sharp Ideas). The ROI benefits of GFI EventsManager are significant in assisting corporations in not losing out when problems related to network security, legal compliance or system health (problems to which no corporation is immune) occur. It acts as a proactive insurance policy that not only protects corporations when regretful incidents occur but actually stops these incidents from happening in the first place. This actively protects corporations from losing money in terms of lost working hours, loss of customers, loss of face and loss of sales.

GFI EventsManager also enables the timely forensic investigation of dubious events by the staff already employed with the corporation. This enables forensic investigation without the costs related to expensive consultancy and audit firms. In itself this also constitutes significant savings for the corporation that, as an added benefit, does not need to wash its dirty linen out in public.

Another benefit that corporations gain by using GFI EventsManager is through employee performance metrics. Through GFI EventsManager, corporations can now monitor employee behavior for performance appraisal purposes. This eliminates ambiguity in a normally grey area of the employee appraisal process by providing clear evidence, through a single console, of employee conduct. It therefore assists corporations in better investing their money and resources where these are most needed.

Conclusion

Through the use of GFI EventsManager, corporations can achieve important goals that are very important to the overall wellbeing of the corporation in terms of legal compliance, information systems security, system health and forensic investigation. Moreover these goals are achieved through the use of technology that is simple to use and which does not necessitate extensive training and technical assistance. Through the "Get Things Done" approach that this software provides, corporations are assured that they are getting not only value for money on their investment but are also adopting best practice principles that pay-off instantly and over a number of years.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

**Disclaimer**

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.