

**“Highest Performance  
Lowest Price”**

**Microsoft**  
**GOLD CERTIFIED**  
Partner

# **GFI** PRODUCT COMPARISON

**GFI EventsManager**  
**VS**  
**Netikus.net EventSentry**

# GFI

## GFI EventsManager vs Netikus.net EventSentry

	GFI EventsManager	EventSentry
Support for MS SQL Server	✓	✓
Support for MSDE / MS SQL Express	✓	✓
Support for MySQL database	✗	✓
Scans and process Windows Event Logs (.evt)	✓	✓
Built in Syslog server	✓	✓
Built in SNMP trap server	✓	✗
Scans and process W3C logs	✓	✗
MS SQL Server audit - C2 style	✓	✗
Processing performance (events/second)	Up to 6000	Around 1000
Requires an agent on each machine	No	Yes
Real time monitoring of events	✓	✗
Machine health monitoring	✓	✓
Noise reduction technology	✓	✗
Out of the box event classification and interpretation for Windows and Active Directory events	✓	✓
Out of the box event classification and interpretation for Linux machines	✓	✗
Out of the box event classification and interpretation for Cisco, Juniper and Allied Telesis network devices	✓	✗
Out of the box event classification and interpretation for Microsoft Exchange Server	✓	✗
Out of the box event classification and interpretation for Microsoft ISA Server	✓	✗
Out of the box event classification and interpretation for Microsoft IIS	✓	✗
Out of the box event classification and interpretation for Microsoft SQL Server	✓	✗
Out of the box event classification and interpretation for PCI DSS compliance	✓	✓
Scan remote sites over WAN links	✓	✗
Role based user authentication in the console	✓	✗
Scans Windows Vista and Windows 2008 Server specific events	✓	✗
Status monitoring available	✓	✗
Notifications via email	✓	✓
Notifications via SMS	✓	✗
Notifications via pager	✗	✓
Specific PCI DSS compliance reports	✓	✓
Account usage reports (ex. failed logons, account lockouts etc)	✓	✗
Account management reports (ex. add/delete/modify users and groups etc.)	✓	✗
Specific reports on changes in domain/local policies/user rights assignment, etc	✓	✗
Specific reports on changes in object access (ex. files, registry etc.)	✓	✗
Scheduled reporting	✓	✗

### Who we are

GFI is a market leader in security software, offering high performance solutions at unbeatable prices to small and medium sized businesses.

Products like GFI MailEssentials, the leading spam filter product on the market, has over 80,000 customers; GFI MailSecurity was the first to apply multiple anti-virus engines to combat viruses; while GFI WebMonitor is the no. 1 web filter for Microsoft ISA Server. GFI FAXmaker remains the best fax server solution around.

GFI leads the way in the SMB sphere, combining price, quality and innovative technology in all products.

### The GFI difference

- More than 30 awards
- Out of the box support for Cisco, Juniper Networks, Allied Telesis network devices
- Smart interpretation and classification of events
- Noise reduction
- Server-based install, no client software required
- Certified for Windows Server 2008



## GFI EventsManager vs Netikus.net EventSentry

### Processing the information ▼ from the extended fields of the Windows events

	GFI EventsManager	EventSentry
Translates cryptic events in reports (such as logon types, privileges codes, access codes, SIDs etc.)	✓	✗
Supports exporting reports to pdf, dox, xls and rtf	✓	✗
More information section added to the description in each event and direct link to website for more info on events	✓	✗

It is not sufficient to process only the general fields of the log messages and archive the extended fields of the event/description in a single field. The information available at the general tags

level (like user, computer, date/time, and event id) is not enough to be able to provide a good granularity when deciding what to do with the message. There are many situations in which the same event, with certain information on an extended field, like object name for object access events, is FAR more important than the same event, with the same general fields, but with different information on the extended field mentioned above. Also, in most of the cases, the extended fields hold the critical information, like the accesses used, logon type, client machine and so on.

At the same time, eliminating noise is a very important aspect of security monitoring. The noise represents in average close to 50% of the data logged, and in some cases even 80%. A good noise reduction system will save you lots of time and resources. Achieving such a good noise reduction system is impossible without the granularity given by the extended fields processing.

Search capabilities on the extended fields is not enough, you also need to match the searched value to a certain extended field. So finding user X in the description of the event, does not mean that user X generated the event. There are events with more than two distinct user names in the description, so it is important to be able to see on which extended field you could find the value User X.

GFI EventsManager achieves the following by using this advanced processing technique:

- higher granularity in interpreting and classifying the events
- faster and easier access to extended event information
- very good noise reduction filters
- accountability for the actions which led to the logging of the events by identifying the user who generated it

### Scanning performance ▼

Having a good scanning performance is the key in ensuring a reliable security monitoring and legal compliancy system, especially in medium to large organizations. At the same time, in order to achieve real time monitoring, you need a high performance scanning engine.

Facts reveal that on average, a domain controller sustaining a domain with a small to medium number of active users and machines generates around 5000 security audits per hour. Domain controllers sustaining larger domains, with 3000+ active users can generate around 130 000 security audits per hour. Add to these numbers the events in the other logs and you will arrive to quite large quantities per domain controller per hour. Multiply the result with the number of Domain Controllers you need to monitor, do the same math for servers,

# GFI

## GFI EventsManager vs Netikus.net EventSentry

workstations, applications and devices you need to monitor, and the final result can be between several hundred thousands and several millions events.

GFI EventsManager offers unequalled scanning and processing performance. Multithreaded scanning, coupled with a medium powered server (dual Xeon at 3.0 GHz and 4 GB of RAM memory) can scan over **6 million events PER HOUR** from multiple log types on multiple machines. This performance should cover most of the performance needs in the SBS market.

### Event interpretation – Best default settings, out of the box functionality

The log messages are very cryptic and little documentation is provided about their meanings. Even less information is provided about all the situations in which the events or sequences of events get generated. Usually people know little both about what they need, and how to interpret the log messages, and the effort to better understand those, takes a lot of time which is usually not available. Just presenting the messages as they are is not a solution for most of the potential users of a security monitoring and legal compliancy solution. What usually happens with regular log management solutions is the following: the software is installed and starts providing a myriad of events which are in the end just numbers. What you need to do is carry out research in order to understand what various numbers mean in order to be able to distinguish important information out of the large quantity of spam. This research may not yield any results in a decent timeframe costing the customer time and leaving him with no solution.

GFI EventsManager offers the best default event processing rules, with intuitive names to serve as translations for the cryptic messages; default computer groups, fully preconfigured in terms of processing rules and actions which apply and scanning intervals, all tailored on computer roles.

Moreover, each security event contains a link to a website where the user can find not only more information on it, but also feedback from a community of users and links to other related information.

The event processing rules system is very flexible and expandable, also allowing fast and easy customization. The importance of having such event processing rules is critical, as they represent both the means, and the knowledge required to successfully perform security monitoring.

### Powerful SQL Audit combined with log management

SQL Audit became a very popular feature among the products which handle log management. There are mainly two ways of auditing the SQL Server: one based on what Microsoft SQL Server logs into the .evt Windows event log, and configuration changes which are determined based on the changes in the system databases, on one hand, and full C2-style auditing which along with the above provides also information on the activity on the user databases.

GFI EventsManager takes the C2-style approach and delivers a full view on what happens on your SQL Server. That means that apart from auditing server/database changes, logons etc, you can also audit activity and know exactly what data was viewed/changed/added, by whom, from what application and from which machine.

### Event processing rules

#### **Why are event processing rules important? How were they created?**

Event processing rules have the following roles: evaluate, interpret, classify, and translate events.

Security related event processing rules and noise reduction rules are created based on the Microsoft Security and Attack Detection Planning Guide, PCI Compliance requirements and "Best Practices" documentation.

The event processing rules for system health, security applications and various computer roles are created based on Microsoft documentation and our vast experience in event log monitoring.

The event processing rules for the Syslog messages received from Cisco devices are created based on extensive research on the vdocumentation provided by Cisco. Same for messages sent by Juniper Networks and Allied Telesis.

The SNMP support included MIBs for most of the important device manufacturers making it even easier for costumers to configure and use the product.

### Database audit

#### **Why is database audit important for compliance?**

Most of the legal compliancy acts ask for the ability to provide accountability for the actions taken when working with sensitive information (cardholder information in case of PCI DSS, financial information in case of SOX, etc). If the sensitive information resides in a database, you will need to audit the activity on that database.

The main problem is that for example, Microsoft SQL Server logs events to .evt format only up to the point where the user is logging on the SQL Server. It does not log any information about the actions which the user performed on user databases. Hence you will need a solution which is able to get this information too.

GFI EventsManager is able to get that information for you. The competition will only be able to collect configuration changes and management information, without any user activity on the user databases.

### Ease of use

#### **How often should I monitor my infrastructure servers?**

#### **What messages should I look for in order to detect a possible attack?**

#### **What system event sources do I need to monitor in order to be alerted on disk failures? What about TCP/IP failures?**

GFI EventsManager answers all those questions for you via its event log management and processing engine. There are preconfigured computer groups and processing rules for those groups, so all you need to do is add your computers or devices to the corresponding computer group in GFI EventsManager.

# GFI

## GFI EventsManager vs Netikus.net EventSentry

### Noise reduction and compliance

#### How much noise is there in the logs?

It is difficult to estimate exactly how much noise the logging systems we support create. For Windows, our research laboratories have conducted tests in order to answer this question. Depending on the audit settings, a computer can generate around 70% noise information as result of: normal system activity/typical behavior, defective logging/bugs and over-logging/redundancy.

For example, instead of getting one event when a user account is created, you get sixteen.

With the retention policies of three month live data, with regards to logs, enforced by the legal compliancy acts, 70% noise is a lot to cater for, and it leads to significantly higher costs to review, store, filter and process noisy events.



#### Disclaimer

The data contained in this document is based on research carried out by GFI. The pricing data for the competitors' products has been compiled from various sources and therefore is correct to the best of our knowledge. GFI does not represent or warrant the accuracy or reliability of this information, and will not be liable if individuals/companies use or misuse this information. Readers should contact directly the companies mentioned in this document to obtain the latest pricing details.