Listen to your data - Log data analysis and IT monitoring made easy

The huge volume of log data generated is an invaluable source of information for system administrators. Managing it effectively helps ensure a reliable network, secure systems and high availability, while aiding organizations with compliance. Real-time network-wide log data management and analysis is needed to achieve adequate security, business continuity and reliability, but with hundreds of thousands of log entries being generated daily, managing them is a challenge.

Increased uptime

Enhanced **Security**

Competitive pricing

GFI EventsManager® eases the burden on administrators and reduces costs. It enables increased uptime by collecting, normalizing, analyzing, categorizing and consolidating log data from multiple sources across the network. It also offers real-time, check-based active IT infrastructure and operations monitoring, making these monumental tasks manageable and allowing a faster, more targeted response to any issue as it arises.

The unique combination of log data analysis with active IT monitoring not only shows you what the problem is, but also helps in identifying the cause of the problem, all from the same console.

BENEFITS

- Protection by detecting and analyzing security incidents through event log data analysis
- Boost your security by monitoring security-relevant activity, mechanisms and applications.
- Cut costs and increase productivity by automating IT management
- Understand what is happening in your IT environment
- Benefit from network uptime and identify problems through real-time alerts and dashboard
- Invaluable companion to help achieve regulatory compliance with SOX, PCI DSS, HIPAA etc.
- Centralized Syslog, W3C, text Windows events, SQL Server and Oracle audits and SNMP traps generated by firewalls, servers, routers, switches, phone systems, PCs and more
- Built-in rules enable out-of-the-box alerting, classification and management of log data

GFI EventsManager™

Log data analysis and IT management

GFI EventsManager also helps you to:

- Gather information from virtually any source at a high level of granularity and depth
- Obtain a detailed view of what is happening across various environments thanks to the variety of log types which are supported
- Track and report on Oracle and SQL server activities such as alteration of DB tables, attempts to access data without necessary privileges, etc.
- Provide reliable data sources for forensic investigations.

GFI EventsManager for security information and event management

GFI EventsManager is able to analyze security-related log data in real time. This way you can detect security incidents and analyze them in detail to find out who is responsible for them. At the same time, you can monitor the configuration, availability and functionality of security-related mechanisms, applications and services as well as related privileged user activity.

GFI EventsManager for IT infrastructure and operations monitoring and management

Using GFI EventsManager you can actively monitor the availability, functionality, usage and performance of your entire IT infrastructure: network protocols, network devices, network infrastructure, servers, services, endpoints and applications, all in real time and from a single console.

You can also monitor firewalls, sensors, routers and the events generated by Microsoft ISA Server, SharePoint, Exchange Server, SQL Server, and IIS, and prevent network disasters from occurring. For example, you can monitor email queues, SMTP gateways, MAPI availability, bad hard disk blocks, disk space and more.

The unique integrated combination of active IT monitoring and log data analysis offers a crucial advantage: Not only do you know when a problem appears (via active IT monitoring) but you immediately gain insight into the cause of the problem as well (via log analysis – you have the relevant log data right there), in the same console.

GFI EventsManager for regulatory compliance

By offering log data collection, normalization and multi-layered consolidation, GFI EventsManager plays an important role in meeting the log data availability retention and reviewing requirements of regulatory bodies and acts including:
Basel II, PCI Data Security Standard, Sarbanes-Oxley Act, Gramm-Leach-Billey Act, HIPAA, FISMA, USA Patriot Act, Turnbull Guidance 1999, UK Data Protection Act, EU DPD.

GFI EventsManager for forensic investigation

Log data is a reference point when something goes wrong, providing a history of detailed information about how electronic systems are used that is often required when you need to carry out forensic investigations due to litigations involving actions carried out via electronic means. GFI EventsManager provides timely in-house forensic investigation capabilities of log data across your network – freeing you of expensive outsourced consultancy and audit costs.

Deeper granular control of events

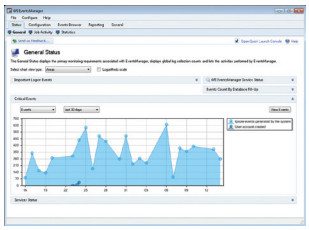
GFI EventsManager helps you monitor a wider range of systems and devices through the centralized logging and analysis of various log types. Administrators can gather information at a great level of granularity, process it at extended tags level and then use the it to take decisions without the need of further information management.

Analysis of network-wide log data

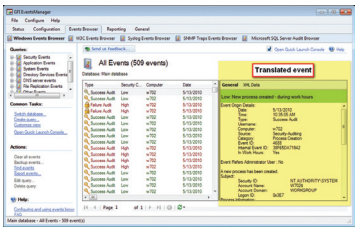
As a network administrator, you have experienced the cryptic and voluminous logs that make log data analysis a daunting process. GFI EventsManager provides network-wide control and management of log data coming from servers (Windows, Linux/Unix, AIX, Mac OS, etc), endpoints (Windows, Linux/Unix, Mac OS), server roles (web servers, database servers, file servers, application servers, remote access servers, virtualization servers etc), applications (any application creating text logs), network infrastructure devices (routers, switches, firewalls), network security appliances (IDS, IPS solutions), generic network-enabled devices (any SNMP-enabled device)

Other features:

- Real-time 24x7 x 365-day log-data monitoring and alerting
- High-performance scanning and storage engines
- Controlled, audited and granular access to log data
- Collection of log data distributed over a WAN into one central database/and/or auto-archiving of all log entries to files
- Rule-based log data management
- Powerful dashboard
- Advanced event filtering features including one-click rule and filter creation
- Reports on key security information happening on your network
- Support for new devices
- Multi-functionality to meet different corporate requirements
- Removal of 'noise' or trivial events
- Scheduling and automated distribution of reports via email
- Events can be exported into customizable HTML files
- Support for virtual environments.



GFI EventsManager management console



Makes cryptic logs easier to understand

System requirements

- Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows Server 2012
- .NET framework 4.0
- Microsoft Data Access Components (MDAC) 2.8 or later

Download your free trial from http://www.gfi.com/eventsmanager

Microsoft Partner
Gold Independent Software Vendor (ISV)

GFI EventsManager™
Log data analysis and IT management

Contact us

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

UK
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

Asia Pacific - South Australia
Tel: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfiap.com

For more GFI offices please visit http://www.gfi.com/company/contact.html

GFI
www.gfi.com