WhatsUp® Log Management

SUPPORTS EVT AND EVTX
Easily open and correlate Windows events generated in a heterogeneous environment from one single console – 2008 and later, XP, Vista, Server 2003, NT 4.0.

INCLUDES PATENTED LOG HEALER TECHNOLOGY
Your solution handles and even repairs corrupted Microsoft EVTX event logs.

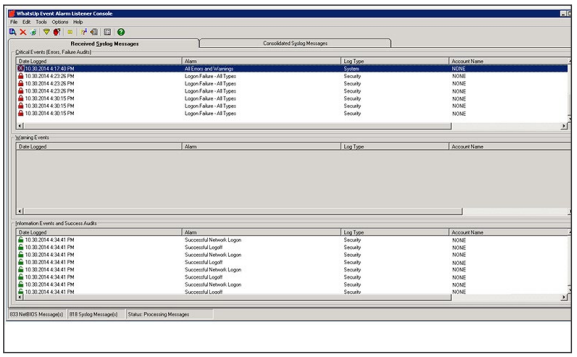
BUDGET-FRIENDLY TIERED PRICE MODEL
No need to keep track of how much log data you generate, no hidden costs if your log files grow, with tiered "per server/workstation" pricing.

Log files contain a wealth of information to reduce an organization's exposure to intruders, malware, damage, loss and legal liabilities. Log data needs to be collected, stored, analyzed and monitored to meet and report on regulatory compliance standards like Sarbanes Oxley, Basel II, HIPAA, GLB, FISMA, PCI DSS, MiFID and NISPOM. Yet, monitoring log files is impossible without the right tools since log files come from many different sources, in different formats, and in massive volumes.

Introducing WhatsUp Log Management Suite

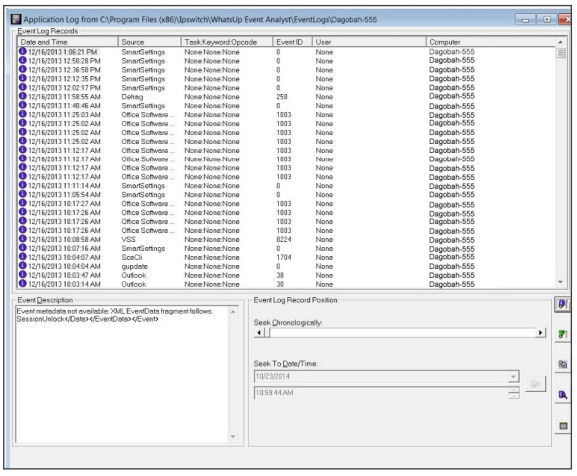
A modular set of applications that can automatically collect, store, alert, analyze and report on Windows Event, W3C/IIS and Syslog files for real-time security event detection and response, and historical compliance assurance and forensics. And, when you integrate the suite with your installation of WhatsUp Gold, you'll have insight into your network and log data from a SINGLE pane of glass.

Event Archiver:
Automate log collection, clearing, and consolidation. Great for assisting in auditing & regulatory compliance.



Event Alarm:
Monitor log files and receive real-time notification on key events. Great for intrusion detection and monitoring for domain controller lock-outs, or file and folder access.

Event Analyst:
Analyze and report on log data and trends. Automatically distribute reports to management, security officers, auditors and other key stakeholders.



Event Rover:
Single console for in-depth forensics across all servers and workstations to increase efficiency and save time.

Log Management ipswitch

- **DOCUMENT AND PROVE** compliance for key compliance initiatives such as HIPAA, SOX, MiFID, etc., with out-of-the-box, point-and-click reporting
- **PROTECT ARCHIVED LOGS** via cryptographic hashing (key for evidentiary use)
- **IDENTIFY UNAUTHORIZED EVENTS** immediately (i.e. access to folders containing sensitive data)
- **COLLECT AUTOMATICALLY** Syslog, Windows Event or W3C/IIS log files across your entire infrastructure
- **STORE LOG DATA AS LONG AS YOU NEED TO** – multi-year data storage capabilities help you comply with key regulations
- **ANALYZE AND EXTRACT** the right information across thousands of log entries
- **REPORT ON CRITICAL ERRORS** or compliance-centric failures right from a WUG dashboard
- **REMOTE & AGENT-BASED COLLECTION** of Syslog, W3C/IIS and Windows Event Files. Log Management adapts to your network security policies, simplifies configuration tasks and saves time

Now IT operations, compliance officers and security personnel can be sure that the WhatsUp Log Management Suite will not only capture and document every event, but also deliver:

- Comprehensive visibility into internal and external security threats
- Automated collection of Syslog, W3C/IIS or Windows Event logs across your entire infrastructure
- Easier regulatory compliance with point-and-click reporting
- Multi-year data storage to comply with key regulations (i.e. HIPAA mandates six years of retention)
- Ability to correlate events from different sources in a single, holistic view
- Protection of archived log data from tampering via cryptographic hashing – key for evidentiary use
- FIPS 140-2 encryption & validation – the highest level of cryptography
- Real-time data views, status and alerting
- Reduced effort to locate and remediate events
- Achieving regulatory compliance at reduced cost