



## LogWatch

It's time you understood your log files. Simplified log management through centralized monitoring, automatic notifications, and powerful search capabilities.

Monitor and consolidate event logs across the IT infrastructure

Quickly pinpoint specific events based on content and event properties with powerful search engine

Receive automatic alerts about critical security and performance events in real-time

Help your compliancy efforts for Sarbanes-Oxley, HIPAA, and others via simplified log management

Streamline IT operations with automated report generation

**What critical information are your log files trying to tell you?** Security breaches, unauthorized access, vital performance statistics- your network constantly generates logs on critical health and security events. And yet, because of their unmanageable numbers and scattered distribution, logs are rarely studied, leaving critical warning signs undiscovered.

LogWatch makes log management a reality for networks of all sizes, bringing essential information to light before it's too late. It consolidates log information from diverse Windows, Unix, Linux, and SNMP sources, as well as provides powerful search and filter functions so you can easily gather the data of interest.

### Flexible and easy to use

LogWatch simplifies log management. It offers a user-friendly, intuitive interface that makes it easy to configure log views and alerts. With just a few mouse clicks, you can select your own view (by type or application).

**LogWatch takes the trouble out of log management. It's easy to deploy and even easier to use.**

You can even change your view and alert settings on the fly; there's no waiting for changes to be updated. Changes can apply to one agent or a group of agents, as needed.

### Detect intruders and security breaches

LogWatch centralizes security and intrusion monitoring across the enterprise infrastructure. It analyzes security event logs for all devices, automatically notifying you of possible breaches in real-time. With LogWatch, you can be confident you have the tools to effectively detect and respond to any misuse, fraud, or intrusions early on.

- Protect your network from internal security threats (critical since firewalls can't protect against this)
- Help protect your Intellectual Property and sensitive data by monitoring access to critical files
- Audit failed access records to prevent larger hacking attempts.
- Know who logs in to which computer, and when.

### Find specific events fast with powerful search and filters

With powerful search methods, LogWatch accelerates log review and analysis. IT staff can quickly pinpoint specific events among thousands of log entries. LogWatch supports flexible search and filter configurations using industry-standard regular expressions. LogWatch searches for specific keywords in log files and then picks up the entire line.

**Active Alerts**

Listing 1 - 5 of 5 results. Page: 1

Alert	Alert Time	Alias	Message	Reactions
	Oct 26th 2006 - 11:20:38 AM	Exchange	Facility 'Exchange' has Information status, this is based on the matched filter: 'MSEExchangeInfo'.	
	Oct 20th 2006 - 8:10:52 PM	MSsql-Prod1	Facility 'MSsql-Prod1' has Warning status, this is based on the matched filter: 'SQLServerWarning'.	
	Oct 20th 2006 - 4:22:33 PM	CapriOSEvent	Facility 'CapriOSEvent' has Information status, this is based on the matched filter: 'SystemEventLogInfo'.	
	Oct 20th 2006 - 4:21:33 PM	LocalWeb	Facility 'LocalWeb' has Error status, this is based on the matched filter: 'SGError'.	
	Oct 03rd 2006 - 8:11:41 PM	MSsql-Prod1	Facility 'MSsql-Prod1' has Warning status, this is based on the matched filter: 'SQLServerWarning'.	

© 2003-2006 NRG Global. All Rights Reserved.

**Message:** This instance of SQL Server has been using a process id of 2080 since 10/13/2006 5:32:53 PM (local) 10/14/2006 12:32:53 AM (UTC). - Event ID: 17177

**Status:**

**Agent:** Capri

**Facility:** DNS

**Matched Filter:** MatchAll

Message Date	Acknowledge Date	Acknowledged By
10-25-06 23:59	N/A	N/A
10-25-06 00:00	N/A	N/A

### Simplify your regulatory compliance efforts

In addition to improving IT operations, LogWatch can help in your Sarbanes-Oxley, HIPAA, and other regulatory compliancy efforts. It simplifies the task of auditing and documenting intrusion detection, network security, and Intellectual Property safeguarding.

### Streamlined report generation

With LogWatch, users can easily generate event log reports. These reports can be sent to all, or a specified list of users. Log reports help fulfill internal process and regulatory requirements, as well as help explain any necessary information to management. By automating report generation, LogWatch frees your valuable IT resources to focus on other proactive or critical IT resources.

### Increase efficiency with multi-user architecture

With LogWatch, multiple users can simultaneously search records, configure filters and notifications, and generate their own reports. This enables each member to focus on his/her own area of interest and responsibility.

### Receive automatic alerts in real-time

LogWatch shortens the time taken to respond to incidents by giving staff immediate access to critical logs. It sends instant alerts to appropriate personnel when key events, like security breaches or performance issues, are detected.

LogWatch is part of the Chroniker Availability Monitoring Suite. All modules monitor from a different perspective:

- SNMP Watch
- Node Watch
- Task Watch
- System Watch
- AppsWatch
- BizWatch

Find out more at:  
[www.chronikersuite.com](http://www.chronikersuite.com)