

# WhatsUp Event Log Management-Suite

## Die wichtigsten Leistungsmerkmale und Funktionen

### Funktionen von Event Archiver

- Automatisierte Erfassung und Speicherung von Windows-Ereignisprotokolldaten
- Kompatibilität mit EVT- und Windows-EVTX-Ereignisprotokollen
- Flexible agentenbasierte und Remote-Erfassung von Windows-Ereignisprotokolldaten
- Automatische Datenbankwartung

### Funktionen von Event Analyst

- Automatisiertes Ereignisprotokoll-Reporting und Korrelieren von Ereignissen
- Leistungsfähige und intuitive Ereignisprotokollkorrelation und -analyse
- Unterstützung von zahlreichen Ereignisprotokollformaten
- Vorkonfiguriertes oder benutzerdefiniertes Ereignisprotokoll-Reporting
- Automatisierte Report-Verteilung

### Funktionen von Event Alarm

- Optimierte Cache-Technik zur Verringerung von Authentifizierungen während des Protokoll-Monitorings
- Überflutungskontrollfunktionen
- Kundenspezifische Domänenenerstellung
- Ping-Test und Offline-Benachrichtigungen
- Benutzerdefinierbare Benachrichtigungszeiten
- Drag & Drop-Konfiguration von Warnmeldungen und Benachrichtigungen
- Detaillierte Syslog-Gerätemeldungen
- Aufzeichnung des zeitlichen Verlaufs des Protokoll-Monitoring

### Funktionen von Event Rover

- Vereinfachte Protokolldatensuche mithilfe von strukturierten Ansichten
- Export von Ereignisprotokolldaten
- Wahrung der Integrität von Protokolldateien während der Überprüfung
- Unterstützung von EVT-X-Protokolldateien
- Erkennung kritischer Sicherheitsvorfälle

## Umfassende Ereignisprotokollierung und -analyse

Die WhatsUp Event Log Management-Suite von Ipswitch ermöglicht Ihnen ein weitreichendes Management jedes Schritts im Lebenszyklus von Ereignisprotokolldaten und gibt Ihnen einen umfassenden Überblick über die Sicherheit und den Zustand Ihrer IT-Infrastruktur.

Durch die lückenlose Kontrolle, die das Ereignis- und Protokollmanagement von Windows-Servern/Windows-Workstations sowie von Routern, Switches, Firewalls, IDS-/IPS-Systemen sowie UNIX-/Linux-Servern gewährleistet, können IT-Mitarbeiter und mit der Sicherheit beauftragte Mitarbeiter zuversichtlich sein, dass jedes einzelne externe oder interne Ereignis, jede Administrations- oder Konfigurationsänderung, jeder Ausfall erfasst und vollständig dokumentiert wird.

### Die WhatsUp Event Log Management-Suite bietet Folgendes:

- Umfassenden Überblick über Benutzer- und Systemaktivitäten
- Echtzeitdatenansicht, -zustand und -Reports
- Unkomplizierte Möglichkeiten, Ereignisse zu lokalisieren und eventuelle Probleme zu lösen
- Automatisiertes Filtern und Indizieren von Protokollen
- Verbesserten Überblick über interne und externe Sicherheit
- Einhaltung behördlicher Vorschriften mit geringerem Kostenaufwand
- Möglichkeit, Ereignisse aus verschiedenen Quellen in Beziehung zueinander zu setzen
- Schutz interner IPs und von Kundeninformationen
- Automatisierte Ereignis- und Protokollmanagementprozesse

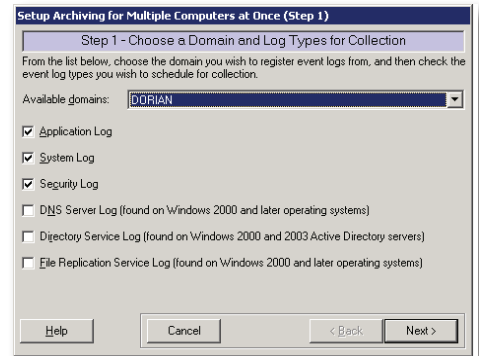
Das Managen von Ereignissen und Protokollen ist in der IT schnell zu einem zentralen Aspekt der Echtzeitforensikanalyse möglicher Sicherheitsprobleme, bei Sicherheitslücken und Server- oder Gerätekonfigurationsproblemen geworden. Darüber hinaus müssen Unternehmen dafür sorgen, dass behördliche Auflagen wie beispielsweise HIPAA, NERC CIP, FISMA, Sarbanes-Oxley, SEC 17(a) und GLB sowie neue Branchenrichtlinien oder Vorschriften lokaler Behörden erfüllt werden, wozu gehört, dass Protokolldateien unmittelbar für Audits hinsichtlich der Konformität mit diesen Bestimmungen verfügbar sind.

Mit der WhatsUp Event Log Management-Suite haben Sie die Möglichkeit, Erfassung, Management, Warnmeldungen und Benachrichtigungen sowie die Archivierung von Syslog- und Windows-Ereignisprotokolldateien zu automatisieren. Die Suite weist außerdem zwei Funktionen auf, die sie von anderen Protokollmanagementprodukten abhebt: Die Log Refiner-Technologie ermöglicht, sowohl mit EVT- als auch mit EVT-X-Protokolldateien zu arbeiten. Die Log Healer-Technologie ermöglicht die Wiederherstellung beschädigter und durch abnormales Herunterfahren fehlerhafter EVT-X-Dateien wiederherzustellen, ohne sie zu ändern und dabei wertvolle forensische Informationen zu verlieren.

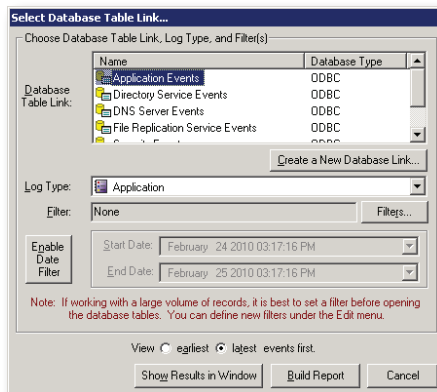
Die WhatsUp Event Log Management-Suite ist mit vielen Betriebssystemen kompatibel, u. a. Windows XP, Windows Server 2003/2008, Vista und Windows 7. Sie wird nicht mit einer Datenbank geliefert; so haben Sie die Wahl, entweder Microsoft SQL Server, Microsoft SQL Server Express oder Oracle zu verwenden. Die Suite beinhaltet vier modulare Lösungen, die separat erworben und ausgeführt werden können.

### WhatsUp Event Archiver

WhatsUp Event Archiver ist eine hochentwickelte Lösung für die Automatisierung von Backup, Konsolidierung und Management von Ereignisprotokollen. Da Event Archiver die Vorgänge des Bereinigens, Erfassens, Konsolidierens und Speicherns von Ereignisprotokolleinträgen aus Remote-Servern und -Workstation rationalisiert, kann sich das IT-Team ganz auf die Analyse der Daten konzentrieren und braucht keine wertvolle Zeit auf ein manuelles Abspeichern von Protokolldateien und deren Management zu verschwenden.



WhatsUp Event Archiver



WhatsUp Event Analyst

### WhatsUp Event Analyst

WhatsUp Event Analyst ist eine fortgeschrittene Lösung zur detaillierten Analyse von Protokolldateidaten nach bestimmten Ereignissen und ermöglicht die Anzeige, Filterung sowie den Export und das Reporting der relevanten Ereignisse. Die Ausführung der in Event Analyst gebotenen vordefinierten Reports kann geplant werden. Dazu brauchen Sie nur Tag und Uhrzeit, einen Ereignisprotokolldatensatz, einen Filter sowie einen Ausgabeordner anzugeben, oder auszuwählen, dass der Report per E-Mail an bestimmte Empfänger gesendet werden soll. Zusätzlich zu den vorkonfigurierten Reports kann das IT-Team auch benutzerdefinierte Reports erstellen, die den speziellen Anforderungen ihres Unternehmens am besten entsprechen.

### WhatsUp Event Alarm

WhatsUp Event Alarm ist eine einfach zu konfigurierende Anwendung für die Netzwerksicherheit, mit der das IT-Team und die mit der Sicherheit beauftragten Mitarbeiter sofort benachrichtigt werden, wenn bestimmte Ereignisse im Netzwerk auftreten. Das Tool überwacht Ereignisprotokolldateien fortwährend und gibt beim ersten Anzeichen von Schwierigkeiten sofort Benachrichtigungen aus. Netzwerksicherheitstechniker können sich auf diese Protokollmanagementfunktionen verlassen, um behördliche Auflagen und interne Sicherheitsstandards zu erfüllen, und zugleich Ressourcen für eine proaktive Netzwerkadministration freisetzen.

### WhatsUp Event Rover

WhatsUp Event Rover ermöglicht ein müheloses Sortieren und Filtern von Protokolldateien in einer strukturierten Ansicht. Diese Funktionalität stellt einen Paradigmenwechsel im Protokolldatei-Management dar, da Ereignisprotokolldateien so schnell anwachsen und eine solch beträchtliche Größe annehmen, dass die alte Praktik, Protokolldateien linear und chronologisch durchzusehen, praktisch als veraltet angesehen werden kann – und das in Netzwerken jeder Größe. Das Tool ist einfach in der Verwendung, ermöglicht das mühelose Anzeigen und Sortieren von Daten und sorgt darüber hinaus dafür, dass ursprüngliche Ereignisprotokollspeicher möglichst nicht beschädigt werden, wenn forensische oder lediglich routinemäßige Überprüfungen der Protokolle ausgeführt werden.

Weitere Informationen zur WhatsUp Gold-Produktfamilie finden Sie unter:

<http://de.whatsupgold.com/products/index.aspx>

Wenn Sie WhatsUp Gold 30 Tage lang kostenlos testen möchten, besuchen Sie folgende Website:

<http://de.whatsupgold.com/products/download/index.aspx>

10 Maguire Road  
Lexington, MA 02421  
(781) 676-5700  
USA

Kingsfordweg 151  
1043 GR Amsterdam  
The Netherlands

Ipswitch Japan 株式会社  
〒106-0047  
東京都港区南麻布4-11-22  
南麻布T&Fビル8階

