



IT vorwärts treiben – mit unübertroffener Einsicht in Netzwerkdaten

IT Teams benötigen relevante Netzwerkdaten in Echtzeit um die richtigen Entscheidungen zu treffen - sowohl kurz- als auch langfristig. EventSentry ist eine leicht zu installierende, hoch verfügbare und skalierbare Überwachungslösung welche die Performance, Compliance und Sicherheit in Ihrem Netzwerk verbessert. Das Preis-Leistungs-Verhältnis ist unübertroffen. Durch eine reibungslose und umfassende Überwachung werden Katastrophen verhindert und Kosten gespart. Neue Benutzer können sich in kurzer Zeit mit EventSentry vertraut machen und die leistungsstarke Überwachungslösung problemlos an Ihre spezielle Umgebung anpassen.

SCHLÜSSELFUNKTIONEN:

- Korrelierung und Überwachung von Ereignisprotokollen und Logdateien in Echtzeit; Überwachung von Leistungsdaten, Festplattenspeicher, Diensten, Prozessen und mehr auf physikalischen und virtuellen (Cloud) Servern und Arbeitsstationen.
- Verfolgen von Prozessen, Konsolen- und Netzwerkankmeldungen, Dateizugriffe, Konten - und Richtlinienänderungen für Regelungen wie PCI, SOX, HIPAA und mehr.
- Datenvisualisierung mit modernen, aufschlussreichen Dashboards und leistungsfähigen Reportingfunktionen. Das mandantenfähige Reporting unterstützt detaillierte Authentifizierung und bietet eine hochentwickelte Suchfunktionalität.
- Unterstützt von zuverlässiger, sicherer (TLS) und komprimierter Datenübertragung über unsichere Netzwerke.
- Einfache Integration von Kernfunktionen mittels existierender oder neuer Skripte in die Überwachungsumgebung.

KUNDENEMPFEHLUNGEN:

- „EventSentry wurde schnell ein essentielles Instrument für die Überwachung von kritischen Infrastruktursystemen“
- „Das Schweizer Taschenmesser von Netzwerküberwachungslösungen!“
- „Skaliert weit besser als konkurrierende Lösungen“
- „Einwandfreie Kundenbetreuung!“
- „Installierung und funktionsfähig in Minuten!“
- „Geht weit über Ereignisprotokollüberwachung hinaus.“
- „Funktioniert genau so wie erwartet.“
- „Einsicht in unsere Systeme war unglaublich.“

Version 3.2

Für weitere Informationen besuchen Sie
www.eventsentry.com



Event Log Überwachung & Korrelation

Echtzeitüberwachung und Korrelation des Ereignisprotokolls mit Unterstützung von Schwellenwerten, wiederkehrende Events, Zeitgeber und mehr.



Compliance Tracking (Richtlinieneinhaltung)

Verfolgt und interpretiert Dateizugriffe, Prozessaktivitäten und Konsolenanmeldungen, erfolgreiche und fehlgeschlagene Netzwerkanmeldungen, lokale & globale (AD) Kontoänderungen, um IT bei der Einhaltung von Richtlinien zu unterstützen.



Logdatei & Korrelation

Überwacht jede Art von Logdatei (z.Bsp. IIS, DHCP, Backup, Firewall) in Echtzeit und verschickt Warnmeldungen basierend auf Filterkriterien. Logdateien können im Reporting abgebildet werden.



Performance

Überwacht jedes Windows® Performance-Objekt und numerische SNMP OIDs. Unterstützt sowohl intelligente Warnmeldungen als auch die langfristige Datensammlung. Bietet auch intelligente Funktionalität wie „Leak Detection“ (z.Bsp. Speicherleck).



Prozess, Dienst und Scheduled Tasks

Proaktive Überwachung von Diensten, geplanten Aufgaben und Prozessen. EventSentry kann auch Prozesse und Dienste automatisch neu starten.



Festplattenkapazität

Komplette Überwachung mit absoluten und relativen Limits von Laufwerken und Verzeichnissen. Trends können mit Diagrammen visualisiert werden und Laufwerksauslastung wird automatisch prognostiziert. Inventar von den 250 grössten Dateien auf jedem Laufwerk.



Zeitsynchronisierung über NTP

Verifiziert und synchronisiert die lokale Zeit mit einem oder mehreren NTP Servern über das NTP Protokoll (basierend auf RFC 1769 und RFC 1305).



Umfangreiche Inventarisierung

Inventarisiert installierte Software, Patches und Hardwareinformationen und virtuelle Maschinen (VMWare® and Hyper-V®). Ermittelt den Garantiestatus für Server von Dell®, HP® and IBM® und zeigt physikalische Ports zu Netzwerk-Switches an.



Sicherheit

Netzwerksicherheit in Echtzeit durch Log-, Datei-(FIM), Dienst- und ARP-Überwachung (erkennt neue Geräte im Netzwerk).



Benachrichtigungen

EventSentry inkludiert 16 verschiedene Benachrichtigungstypen, inklusive: SMTP Email, Syslog, SNMP Traps, HTTP(S), Jabber (IM), Datenbank, SNPP, RSS, Textdatei, Prozesse, Reboot, Dienstkontrolle, Desktop und mehr.



Unsichtbare Überwachung

Unsere Agenten überwachen Ihre Server & Workstations mit minimaler Netzwerkauslastung und ohne die Leistung der überwachten Hosts zu beeinträchtigen.



Zentraler Kollektordienst

Ein zentraler Kollektordienst unterstützt Komprimierung und Verschlüsselung der Daten über unsichere Netzwerke (z.Bsp. Internet) mit Hilfe von sicherem TLS. Ein lokaler Cache bietet hohe Verfügbarkeit, vor allem bei mobilen Geräten wie Laptops.



Web Reporting

Web Reporting der nächsten Generation mit Dashboards, Zugangskontrolle, flexibles Reporting, Job-Engine und vielen visuellen Darstellungsmöglichkeiten. Ein umfassendes API ermöglicht den Zugriff auf alle Daten mit Hilfe externer Software. Funktioniert mit allen gängigen Web-Browsern und Mobilgeräten.



Netzwerküberwachung

Zentrale Überwachung von Hosts über ICMP und TCP mit detailliertem Status und Historie.



Syslog/SNMP/ARP-Daemon

Zentrale Sammlung von sowohl Syslog Nachrichten als auch SNMP Traps (v1-v3) von Unix/Linux Hosts und/oder Netzwerkgeräten. Warnmeldungen können in Abhängigkeit von Filterkriterien in Echtzeit verschickt werden.



Uptime

Ermittelt die aktuelle Laufzeit von Servern und erstellt eine „Rebootgeschichte,“ um problematische Server, die zu häufig neu gestartet werden, zu identifizieren. Speichert auch die längste Laufzeit von jedem überwachten Gerät.