EVENTSENTRY

Know when you need to act.

Delivering meaningful insight into your network data.

EventSentry is a powerful monitoring solution that provides your IT team with actionable network data that drives intelligent IT decisions – in real-time. Reliable, secure, scalable, and easily-deployed, EventSentry will enhance the performance, compliance and security of your network. Save time, prevent disasters and reduce TCO with one of the most cost-effective monitoring solutions on the market. New users are up and running in minutes and can easily adapt the solution to suit their needs - with award-winning customer service at their fingertips.

KEY FEATURES:

- Correlate and monitor event logs and log files in real time as well as monitor performance, disk space, services, processes and much more on both physical and virtual (cloud) servers and workstations.
- Track Active Directory™ changes of any object down to the attribute level, including group policy changes. Detect compromised & duplicate passwords. Includes user status reports and password expiration reminders for end users.
- Ready to use compliance reports and dashboards - powered by a security engine geared for Windows™ help jumpstart various compliance requirements like PCI, CMMC, NIST & CJIS.
- Visualize data with insightful dashboards and a powerful job & reporting feature. Reporting supports granular authentication and sophisticated log searching.
- Automated Security, Compliance & Hardening scripts increase security, reduce the attack surface and validate compliance settings.

CLIENT RAVES:

"EventSentry has quickly become an essential tool in monitoring the health of critical infrastructure systems."

"The Swiss Army knife of Networking Monitoring solutions!"

"Scales well beyond the competition."

"Their customer service has been impeccable!"

"We were up and running in minutes!"

"Far and beyond event log monitoring."

"It works like it's supposed to."

"Visibility of our systems was mind-blowing."

Version 6.0

For more information call 312.624.7698
www.eventsentry.com

Features Overview

EVENTSENTRY

Event Log Monitoring & Correlation

Real-Time event log monitoring & correlation with anomaly detection and advanced features such as thresholds, recurring events, timers, lateral movement detection, threat scoring and more.

Compliance & Security

Track file/registry/process activity, console logons, successful or failed network logons, account management and more to help with PCI, CMMC, NIST, CJIS and other compliance requirements. Automatically manage Sysmon network-wide.

Log File Monitoring & Correlation

Monitors and correlates any log file (e.g. IIS, DHCP, Backup, Firewall) in real-time and sends alerts upon matching text. Create custom views for structured log files.

NetFlow

Visualizes and enhances NetFlow and sFlow data with GeoIP, threat intel and port scan detection. Sysmon integration correlates process network activity with NetFlow.

Extensive Inventory

Inventories installed software, browser extensions, patches as well as hardware information, including VM inventory (VMWare© and Hyper-V©). Shows physical switch port mappings and managed hardware info.

Comprehensive System Health Monitoring

Keeps track of all important system metrics like disk & folder usage, performance metrics, reboots, critical OS files and more.

Processes, Services & Scheduled Tasks

Pro-actively monitors services, scheduled tasks and processes. Extensive tracking & monitoring of process activity (may require Sysmon).

Notifications & Remediation

Send real-time notifications via email or Web APIs, forward logs via Syslog, send SNMP traps, automatically remediate with custom processes, scripts, reboots, service control and more.

Deep Active Directory Monitoring

Tracks AD object changes down to the attribute level including before & after values, group policy changes, user status reports & password expiration emails. Identifies compromised and duplicate passwords.

Permission Inventory

A searchable NTFS permission inventory of select folders that allows to quickly identify access and audit permissions assigned to users and groups.

Intelligent & Lightweight Agents

Agents monitor your hosts without affecting the performance of the monitored hosts, while also minimizing network bandwidth usage. Agents can be automatically installed and have no dependencies.

Automated Security, Compliance & Hardening

Collection of customizable security and health scripts detect insecure settings, missing patches and updates, compliance violations and misconfigurations on monitored servers and end points.

Web Reporting

Modern web-reporting with dashboards, granular access control, flexible reporting, jobs engine and visualization tools. Extensive API to access data from 3rd party software. Works with all major browsers and mobile devices.

Heartbeat Monitoring

Centrally monitors the uptime of hosts and TCP services and provides availability stats.

Syslog/SNMP/ARP Daemon

Collects Syslog messages and SNMP traps (v1-v3) centrally from Unix/Linux hosts and/or network devices. Alerts matching configured rulesets can be dispatched in real-time.

FIM: File Integrity Monitoring

Tracks checksums, size, version, entropy and digital signatures of critical files to detect & track changes. Real-time alerts and reporting support compliance security requirements.

Version 6.0

For more information call 312.624.7698
www.eventsentry.com