ManageEngine
EventLog Analyzer

Success Stories

Pulling Up the SOX!

ManageEngine EventLog Analyzer enables TRC Companies, Inc. to successfully achieve SOX Compliance

Initial deployment, log collection and SOX compliance report creation completed in hours!

OVERVIEW

Industry

Environmental Services

Critical Requirements

- Ensure 100% connectivity & uninterrupted functioning of data centers and offices
- Collect, analyze and archive huge volumes of real-time logs
- Generate comprehensive reports for SOX compliance audits
- Detect suspicious activities in the Network that could lead to breach of data

Solution

ManageEngine EventLog Analyzer

Results

- Canned SOX Compliance reports met the auditors stringent requirements
- Real time alerts on suspicious activities
- All network activity & logs are monitored 24x7

The Customer

TRC is a national engineering consulting and construction management firm providing integrated services to the energy, environmental and infrastructure markets. They serve a broad range of clients in government and industry, implementing complex projects from initial concept to operations.

Environment

TRC has 2400+ employees spread over 70 offices and has two data centers in Arizona and New Jersey to handle the network load. Their environment consists of 40 to 50 domain controllers, 400+ Web servers, several Cisco devices (firewalls, IPS, switches, routers, etc…), ERP, Microsoft Exchange Server, Microsoft SharePoint, virtual machines, thousands of desktops (Windows, Linux) SAN storage and other business critical hardware.

Their network operations team has to ensure 100% connectivity and uninterrupted functioning of their data centers and offices. As a public company, TRC's network operations team also has an additional responsibility of collecting, retaining, and reviewing terabytes of audit trail logs, generated by their network infrastructure, to support IT process controls of Section 404 of the Sarbanes-Oxley (SOX) Act.

Key Requirements

TRC's network operations team was looking for:

- A vendor agnostic solution that can handle system logs from a variety of hardware
- A solution that can collect, analyze and archive huge volumes of real-time logs
- A solution that instantaneously sends alert notifications for anomalous network behavior
- A solution that provides comprehensive reports for SOX compliance audits

"We chose ManageEngine EventLog Analyzer over other solutions because it was the only solution that provided us with predefined report templates for Sarbanes-Oxley (SOX) Act which helps us meet our audit requirements."

Devank Kumar,
Manager Enterprise Systems & Network Security,
TRC Companies, Inc.

The Solution

ManageEngine EventLog Analyzer
After evaluating several solutions in the market like GFI, Orion, and others, TRC finally chose EventLog Analyzer as their appropriate solution. One of the most critical requirements for TRC was to provide their auditors with comprehensive SOX audit reports based on management assessment of internal control. EventLog Analyzer lets TRC collect, retain and review terabytes of audit trail log data from all sources to support IT process controls of Section 404, Sarbanes-Oxley Act.

These logs form the basis of the internal controls that provide enterprises like TRC with the assurance that financial and business information is factual and accurate. EventLog Analyzer's SOX reports cover sections 302 (a)(5)(A), 302 (a)(4)(C), 302 (a)(4)(B), 302 (a)(4)(A), 302 (a)(4)(D), 302 (a)(5)(B), 302 (a)(6)

EventLog Analyzer also met with their other critical requirements, including:

- Ease of deployment
- Ease of use to achieve quicker time to value and better adoption
- Ability to process a wide range of system and application logs
- Support for other regulatory compliance reports like HIPAA, PCI, GLBA, etc…
- Automatic scheduling of reports
- Ad Hoc reporting capabilities for Security Information Event Management
- Availability of real-time phone and email support and rapid responses to queries to ensure minimal down time
- Lower TCO with minimal investment in additional hardware

Key Results

- Deployment was completed under an hour and log collection was almost instantaneous
- The first set of reports were available to system engineers almost immediately
- The canned SOX Compliance reports met their auditors stringent requirements
- EventLog Analyzer GUI was so user friendly that network operations team were able to effortlessly generate their own reports without any technical assistance
- Network anomalies and aberrant behavior were easily detected
- The availability of SMS and Email alert notification allows the operations team to immediately respond to security threats
- The significant amount of IT operations time that EventLog Analyzer saves for TRC has enabled them to focus on efficiently managing their production environment, handle complex configuration management challenges

About EventLog Analyzer

EventLog Analyzer is a web based, real time, agent less/ agent-based, event log and application log monitoring and management software. EventLog Analyzer helps monitoring internal threats to the enterprise IT resources and tighten security policies in the enterprise.

https://forums.manageengine.com/eventlog-analyzer http://www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine is the leading provider of cost-effective enterprise IT management software and the only one making the 90-10 promise - to provide 90 percent of the capabilities offered by the Big 4 at just 10 percent of the price. More than 50,000 organizations in 200 countries, from different verticals, industries and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of Zoho Corp.