

EventLog Analyzer

“The best thing, I like about the application, is the well structured GUI and the automated reports. This is a great help for network engineers to monitor all the devices in a single dashboard. The canned reports are a clever piece of work”

*Joseph Graziano MCSE CCA VCP,
Senior Network Engineer, Citadel*



About Citadel

Citadel is a full-service financial institution with products ranging from insurance and investments to money market and checking accounts. Its mission is to identify and meet their customers' needs through a full range of financial and insurance services, while maintaining financial safety and soundness.

Citadel was established in 1937 as the Lukens Steel Company Employees Credit Union. In 1983, it expanded its charter to become a community credit union. Today, it has more than 100,000 members, and over \$1 billion in assets.

Citadel's Security Challenge:

Banking and financial institutions are at a greater IT security risk than other companies. They have to ensure the security of the data and other IT resources in their environment. Additionally, government imposes a set of regulations for these companies to comply with. As part of the assurance of the data and IT resources security, Citadel's network engineer wanted to monitor the audit logs of the Administrator users in particular, on critical servers in the network.

The Network Engineer had the huge manual task of finding the critical Audit log events. In particular, audit logs clearing events and audit policy change events on the Citadel's servers are very critical for security. Prior to deploying ManageEngine solution, they used generic tools like spread sheets to examine the error logs. Joseph Graziano, Senior Network Engineer at Citadel explained the challenge Citadel was facing as, "Before using EventLog analyzer we manually captured event logs from our servers into spreadsheets and had daily checklists to examine these for errors. As you can imagine this was a very long and tedious task"

ManageEngine's Solution:

ManageEngine EventLog analyzer can pin-pointedly track the specific critical events like the Audit logs, which the Citadel wanted to track. With continuous, automated monitoring of such events, it can generate alerts and notify the network engineer in real-time. Apart from the alerts, it can provide exhaustive reports for the selected critical events. This is what Joseph Graziano, Senior Network Engineer at Citadel has to say about the EventLog Analyzer solution, "EventLog Analyzer reports are very helpful for audit purposes. The features, real-time graphs of events, search capabilities and drill down to specific events, are very useful".

Benefits to Citadel

The important business benefit of EventLog Analyzer deployment is the elimination of manual log analysis. This saved a lot of time for the network engineer to concentrate on other critical security issues and chalk out contingency plans to mitigate them. “It has just eliminated my manual work”, Joseph Graziano, Senior Network Engineer at Citadel spoke about the benefits of the EventLog Analyzer product deployment. He further went on to add, “We are a financial organization so compliance is a large part of what we do on a daily basis. The reporting and searching capabilities of EventLog Analyzer greatly help us to provide top notch reporting to our auditors”. EventLog Analyzer offers Compliance reports and a list of other features, which will lighten the burden of the network engineer.

About Eventlog Analyzer

EventLog Analyzer is a web-based, agent-less syslog and windows event log management solution that collects, analyzes, archives, and reports on event logs from distributed Windows hosts and, syslog from Linux/UNIX hosts, Routers & Switches, other syslog devices and selected applications. EventLog Analyzer helps organizations to adhere to the demands of regulatory compliance requirements like PCI-DSS, HIPAA, FISMA, SOX and GLBA. With 2800 satisfied customers who include several Fortune 500 companies, the benefits that EventLog Analyzer offers are multifold.

Rating the Product

“I looked at other log monitoring solutions as well but ultimately decided to go with Manage Engine. It beats all of them with its variety in offerings and its reasonable price. EventLog Analyzer is definitely worth the investment. I would rate the product a 10 out of 10”

Joseph Graziano,
Citadel's Senior Network Engineer

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. The ManageEngine suite offers enterprise IT management solutions including Network Management, HelpDesk ITIL, Bandwidth Monitoring, Application Management, Desktop Management, Security Management, Password Management, Active Directory reporting, and a Managed Services platform. ManageEngine products are easy to install, setup and use and offer extensive support, consultation, and training. More than fifty thousand organizations from different verticals, industries, and sizes use ManageEngine to take care of their IT management needs cost effectively.

Website : www.eventloganalyzer.com

Email : eventlog-support@manageengine.com

Toll Free : +1 888 720 9500

Forums : <https://forums.manageengine.com/eventlog-analyzer>

ManageEngine® (A Division of ZOHIO Corp) 4900 Hopyard Rd., Suite 310, Pleasanton, CA 94588, USA.

Website: www.manageengine.com

Email: eval@manageengine.com