

Citadel Bank uses ManageEngine® EventLog Analyzer for Privileged User Monitoring and Auditing (PUMA)

EventLog Analyzer helps Citadel bank to monitor internal user activities and ensure data security

OVERVIEW

Industry

Banking

Critical Requirements

- Ensure data security and network security within the Bank
- Monitor audit logs of users with Administrator privileges
- Analyze log data for regulatory compliance and security purposes

Solution

ManageEngine EventLog Analyzer

Results

- Completely eliminated manual effort of analyzing logs
- Privileged User Monitoring and Audit (PUMA) and Reporting is now available
- Stays compliant with various government regulatory audits
- Real time alerts on suspicious activities

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"



“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

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.

"I looked at other log monitoring solutions as well but ultimately decided to go with ManageEngine. 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 EventLog Analyzer

EventLog Analyzer is a web based, real time, agent less (optional agent available) 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.

ManageEngine is a trademark of ZOHOO Corporation. All other brand names and product names are trademarks or registered trademarks of their respective companies.