

ManageEngine EventLog Analyzer

The ManageEngine EventLog Analyzer from Zoho Corp. is a small application that provides a lot of functionality. This product takes an agentless approach to collecting and analyzing machine-generated logs. The tool can collect and normalize event logs and machine data and make them available for analysis, searching, report generation and archive, all in an easy-to-use, web-based interface.

We found installation to be just about as simple as it gets. The installation executable can be downloaded from the ManageEngine website. Once we had the executable, we ran it on one of our Windows servers and, after a short installation wizard, we were up and running. The product itself is quite small and lightweight, so it can sit on almost any hardware. After the install was complete, we were able to access the web-based management interface. We found this interface to be a little overwhelming at first, but after a few minutes of wandering around we felt pretty comfortable using the controls.

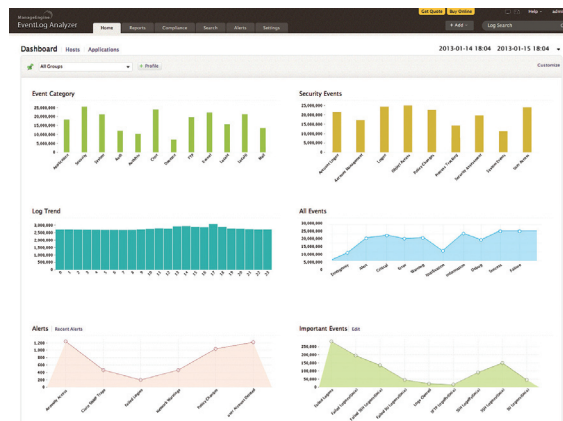
Adding assets and log sources is quite easy as well. This product can scan an entire subnet or devices can be added manually. In our Windows domain environment, we just had to provide administrator credentials and scan our subnet and we were collecting data in minutes. As for analysis, this product features many charts and graphs in its default dashboard that provide a good overview of what's happening around the network. However, for a more detailed view, this product comes preloaded with report templates, including many compliance-based reports.

Documentation included a single help file that is built into the management interface itself. We found this to be quite detailed for a help file. It actually felt more like an administrator guide. It included many screen shots, diagrams and step-by-step configuration and management instructions in a well-organized format. While we did not receive any other manuals, we found that this file did an exceptional job of providing the necessary information to configure and use the product.

ManageEngine provides no-cost support for the first 30 days of product use. After that, customers on the perpetual license model must purchase support as part of a maintenance contract. Customers with a subscription model price have assistance included in their subscription cost. Customers receive email- and phone-based technical support, as well as access to a large online aid area. Customers who access the online support will find a knowledge base, user forum, product video tutorials, documentation and other resources.

At a price starting at \$1,995 for 25 hosts (perpetual) or \$795 per year for 25 hosts (subscription), we find this product to be a good value for the money. The EventLog Analyzer provides some very solid SIEM functionality at a reasonable cost for smaller environments that want to get started with SIEM, but can't afford to invest in a full-scale product. Overall, we find this solution to be easy to deploy and manage in any size environment and to have a solid price for the feature set.

– Peter Stephenson, technology editor, SC Magazine



DETAILS

Vendor Zoho Corp.

Price Starts at \$1,995.

Contact manageengine.com

Features ★★★★★½

Ease of use ★★★★★

Performance ★★★★★½

Documentation ★★★★★

Support ★★★★★

Value for money ★★★★★

OVERALL RATING ★★★★★

Strengths Easy to deploy for smaller environments.

Weaknesses Device and log support is limited.

Verdict Good choice if it supports your environment.



ManageEngine - A division of Zoho Corporation
 4900 Hopyard Rd., Suite 310, Pleasanton, CA
 94588, USA
 Phone: +1 888 720 9500
 Fax: +1-925-924-9600
 eFax +1-925-369-0436
 Email: sales@manageengine.com

