

SIEM

Your Complete IT Security Arsenal

Why Should Enterprises Choose EventLog Analyzer as Their SIEM Solution?

Joel John Fernandes

Author and SIEM Expert



ManageEngine
Powering IT ahead

©2014 ZOH0 Corp, Inc. All Rights Reserved



Introduction

Security Information and Event Management (SIEM) solutions provide enterprises with network security intelligence and real-time monitoring for network devices, systems, and applications. Using SIEM solutions, IT administrators can mitigate sophisticated cyber attacks, identify the root cause of security incidents, monitor user activity, thwart data breaches, and, most importantly, meet regulatory compliance requirements.

The IT infrastructure of any enterprise includes network devices (routers, switches, firewalls, etc.), systems (Windows, Linux, etc.), and business-critical applications that generate a huge amount of log data. This log data can provide powerful insights and network security intelligence into user behaviors, network anomalies, system downtime, policy violations, internal threats, etc.

Meeting your IT security requirements by manually analyzing the log data is impossible because the volume of log data is enormous. Real-time log monitoring and analysis cannot be achieved if done manually. Therefore, automation is the key to leveraging log data, and that's where SIEM solutions come in.

In this handbook, we'll discuss the challenges that IT administrators face while managing terabytes of log data to ensure IT security. We'll also discuss 14 critical capabilities common to most SIEM solutions and how the ManageEngine EventLog Analyzer SIEM solution can help enterprises meet their IT security needs effectively. Finally, we'll list the business benefits an enterprise can gain when it deploys a SIEM solution.

Using SIEM solutions, IT administrators can mitigate sophisticated cyber attacks, identify the root cause of security incidents, monitor user activity, thwart data breaches, and, most importantly, meet regulatory compliance requirements.

Log Management Challenges

We'll now discuss some key log management challenges that enterprises face.

Analyzing Logs for Relevant Security Intelligence

Analyzing information in real time from terabytes of log data is the greatest challenge that network administrators face. Moreover, manual analysis and correlation of log data for IT security is difficult and prone to human error. Therefore, administrators need to rely on automated solutions to analyze huge amounts of log data generated by their network infrastructure. Administrators need to be notified in real time when anomalies occur in applications, systems, and devices. Automated tools can also help administrators identify suspicious user activities on the network.

Centralizing Log Collection

Collecting log data from heterogeneous sources (Windows systems, Unix/Linux systems, applications, databases, routers, switches, firewalls, etc.) at a central place can be a daunting task for IT administrators. Log collection is done by using agents or through an agentless mechanism. Using agents or not using them totally depends on the security policies charted by the organization. Using multiple tools to manage different log formats from numerous devices, systems, and applications is not an effective way to manage the logs in an enterprise. IT administrators need a single, centrally located tool that allows them to decipher any log format from any source.

Meeting IT Compliance Requirements

IT administrators want compliance auditors to finish their work with minimal effort. Verbal assurance to compliance auditors is never sufficient. Compliance reports have to be ready, and the reports must be backed up with the appropriate log data and with the data management tools used. Meeting compliance requirements laid down by regulatory bodies such as FISMA, PCI DSS, SOX, HIPAA, ISO 27001, etc. is impossible without effective log management and compliance tools. Therefore, enterprises are now proactively moving towards demonstrating compliance, because a secure IT network results in improved quality of service and competence of the enterprise, enhanced brand value, and customer satisfaction.

Conducting Effective Root Cause Analysis

Searching through logs to find the root cause of a network problem or spotting a pattern in events is like finding a needle in a haystack. IT administrators find it very difficult to get answers to their questions when they need them the most. They need search capabilities that would enable them to conduct log forensics, which will help them find and remediate network issues and anomalous behavior quickly. Log search capabilities should give the network administrator the freedom to search across the network infrastructure.

Making Log Data More Meaningful

Network administrators need better data representation in different graphical formats, reports, and dashboards. Viewing and analyzing log data graphically is usually preferred. Instead of sifting through raw log data and gaining intelligence, the administrator must be able to make decisions just by glancing at the graph report. The dashboard is among the most critical components of an IT security solution. It is the primary interface to monitor real-time events and perform log data analysis. Presenting vital information from the log message in the form of graphs and charts is essential to help administrators take timely action.

Tracking Suspicious User Behavior

Data thefts, outages, and system crashes can be caused by your most trusted employees and users who have privileged access to business-critical applications, devices, systems, and files. Confidential data can be misused, which can lead to hefty monetary losses for enterprises. IT administrators find it difficult to monitor user activities in real time across the IT infrastructure. Enterprises need real-time monitoring and notifications when anomalous activity occurs on their network devices, applications, systems, files, and more.

Archiving Logs Centrally

Archiving logs centrally is a mandate for all enterprises to meet compliance requirements. Log archiving depends of the policies laid down by the enterprise and the regulatory compliance it follows. The log archiving period varies according to the compliance audit. For example, PCI DSS requires 1 year, HIPAA requires 7 years, FISMA requires 3 years, etc. Another good reason for archiving logs in a central place is for log forensic investigation. Also, archived log data must be protected from changes to ensure authenticity.

Why SIEM?

In today's business environment, IT infrastructure is considered the lifeline of any organization, both large and small. And, keeping the IT infrastructure secure from threats has become a difficult task for IT personnel. Log data that is generated by network systems, devices, and applications is a gold mine that can help organizations keep their network secure from all network threats; that is, only if the log data is monitored and analyzed in real time.

Organizations need tools that can derive meaningful, actionable information, and security intelligence from the log data. Monitoring and analyzing log data is not a one-time process that will secure your network. It should be an ongoing process in which the log data is collected, monitored, and analyzed in real time at a central location.

Security information and event management (SIEM) solutions have entered the market to provide security intelligence and automate managing terabytes of log data for IT security. SIEM solutions monitor network systems, devices, and applications in real time, providing security intelligence for IT professionals to mitigate threats, correlate events, identify the root cause of security incidents, and meet compliance requirements.

SIEM Product Alert

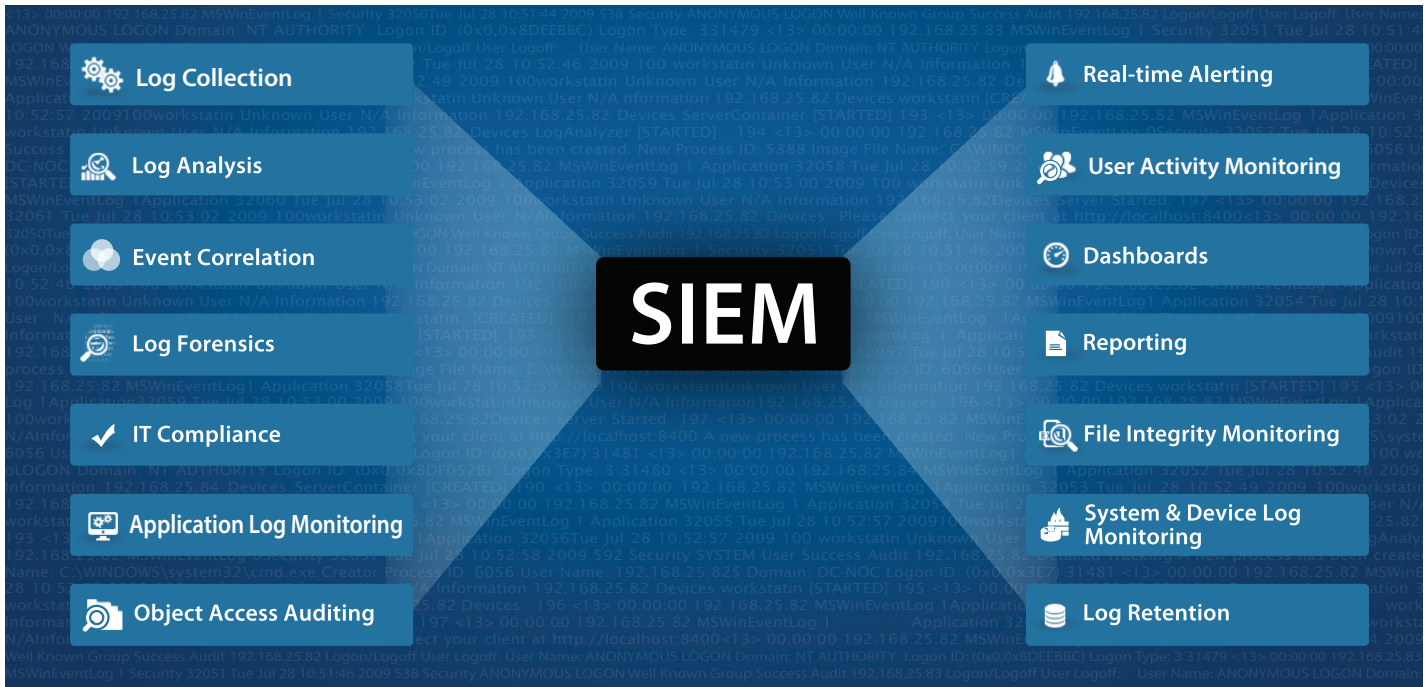
ManageEngine EventLog Analyzer SIEM


EventLog Analyzer SIEM provides the most cost-effective Security Information and Event Management (SIEM) software on the market. It allows organizations to automate the entire process of managing terabytes of machine-generated logs by collecting, analyzing, searching, reporting, and archiving data from one central location.


IT security professionals can now mitigate threats, conduct log forensic analysis, monitor user activity, and comply with different compliance regulatory bodies by using a single tool. The EventLog Analyzer SIEM software provides organizations with complete visibility into their network infrastructure to keep their network secure from threats in real time.


Critical Security Information and Event Management (SIEM) Capabilities

Let us now see the 14 critical capabilities that make an SIEM solution effective and how ManageEngine's EventLog Analyzer SIEM provides all the capabilities in a single SIEM solution.



 Log Collection	EventLog Analyzer SIEM Advantage
<p>A SIEM solution should have the capability to aggregate logs from heterogeneous sources (Windows systems, Unix/Linux systems, applications, databases, routers, switches, and other devices) at a central location. Universal log collection is a critical requirement for enterprises looking out to deploy a SIEM solution.</p> <p>The advantage of the universal log collection feature is that enterprises will be able to collect and analyze any log data format from any source. Moreover, the log collection method (agent-based or agentless) is also an important aspect of the SIEM solution. However, using agents or not using them totally depends on the security policies the enterprises follow.</p>	<p>The EventLog Analyzer SIEM aggregates logs from heterogeneous sources (Windows systems, Unix/Linux systems, applications, databases, routers, switches, etc.) at a central location. It also supports universal log collection through its Universal Log Parsing and Indexing (ULPI) technology, which enables you to decipher any log data, regardless of its source and format. Although most log data from a network infrastructure can be collected through the agentless method, EventLog Analyzer SIEM offers agent technology as well to meet the diverse requirements of enterprises.</p>

 Log Analysis	EventLog Analyzer SIEM Advantage
<p>Analyzing raw log data and generating intelligence for IT security in real time should be the core of any SIEM solution. The raw log data should be analyzed and relevant actionable security data should be represented in easy-to-understand charts, graphs, and reports. IT administrators should easily drill down through log data shown on the dashboard for more insights on user activity, network threats, event trends, and more within minutes.</p>	<p>The EventLog Analyzer SIEM analyzes the log data from your network devices, systems, and applications in real time, enabling IT administrators to mitigate threats and detect network anomalies. The actionable security data is presented as graphs and charts on the dashboard. You can quickly drill down the data on the dashboard and perform a root cause analysis to identify why a security activity happened. IT administrators can also generate security reports at any given time due to real-time log analysis.</p>

 Event Correlation	EventLog Analyzer SIEM Advantage
<p>Real-time event correlation is all about proactively dealing with threats. Correlation of events allows network administrators boost their network security by processing millions of events simultaneously to detect anomalous events on the network.</p> <p>Correlation can be based on log search, rules, and alerts. Network policies can be used to frame the correlation rules and alerts. Most SIEM vendors provide event correlation capability based on rules, and some vendors focus on correlating events by using log search scripts and alerts.</p>	<p>The EventLog Analyzer SIEM provides a powerful correlation engine that you can use to mitigate threats proactively. It includes predefined correlation rules based on threshold conditions or anomalous events, which can be customized.</p> <p>The IT administrator is notified in real time during any threshold violations or network anomalies by an SMS or email. The advanced log search feature provided by EventLog Analyzer SIEM also allows for multi-event correlation, wherein the IT administrator can do a root cause analysis by correlating multiple events and attributes.</p>

 Log Forensics

EventLog Analyzer SIEM Advantage

SIEM solutions help security professionals conduct log forensic investigation by allowing them to conduct a root cause analysis to track down a network intruder or the event activity that caused the network problem. The log forensic process should be very intuitive and user-friendly, allowing IT administrators to search through the raw log data easily. Log search queries once entered by the IT administrator should quickly pinpoint the exact log entry that caused the security activity, find the exact time of occurrence, the person who initiated the activity, and the location from where the activity originated.

The EventLog Analyzer SIEM makes forensic investigation very easy with its powerful log search functionality and instantly generates forensic reports based on the search results. It provides two different log search capabilities, the Basic Search and the Advanced Search. Basic Search permits users to use wild cards, phrases, and Boolean operators while framing the search query. Grouped searches and range searches can also be conducted by using Basic Search. EventLog Analyzer SIEM's Advanced Search has much more sophisticated search capabilities, but retains the ease of basic search.


 IT Compliance


EventLog Analyzer SIEM Advantage

SIEM solutions are incomplete without IT compliance reporting capabilities. SIEM solutions provide out-of-the-box regulatory compliance reports for various regulatory compliance standards, such as PCI DSS, FISMA, GLBA, SOX, HIPAA.

To meet compliance requirements, organizations need to monitor their network in real time, ensure high levels of security for their confidential assets, and provide network audit reports to auditors when needed.

With EventLog Analyzer SIEM, administrators can gain better insights into security threats and meet regulatory compliance requirements by monitoring and analyzing log data from the network infrastructure. Security professionals can now generate pre-defined/canned compliance reports such as PCI DSS, FISMA, GLBA, SOX, HIPAA, etc. within minutes. The EventLog Analyzer SIEM allows users to customize the existing out-of-the-box compliance reports to meet their specific internal audit requirements. It also allows IT administrators to generate new compliance reports to comply with the new regulatory acts, which may demand compliance in the future.

 Application Monitoring	EventLog Analyzer SIEM Advantage
<p>IT administrators need to monitor effectively the logs of their business applications such as databases, DHCP servers, web servers, etc. Network hackers can easily gain access to business applications and cause a data breach if the business applications are not monitored in real time. SIEM solutions should allow IT administrators to monitor their business-critical applications in real time and detect anomalies/suspicious activities on their network applications.</p>	<p>EventLog Analyzer SIEM allows IT administrators to monitor their business-critical applications in real time. It also helps IT administrators proactively detect anomalies/suspicious activities. IT administrators can also generate security reports for their applications and get precise details of the top events generated, event trends, and more. Using these security reports, administrators can easily determine errant users and abnormal behavior of applications, reducing the troubleshooting cycle. You can also analyze and generate reports for any log data collected from your in-house/proprietary applications by using the Universal Log</p>

 Real-time Alerting	EventLog Analyzer SIEM Advantage
<p>Real-time alerting is a mandate for all SIEM solutions and should alert IT security professionals when network anomalies and suspicious activities occur on the network. IT administrators need to monitor, detect, and respond in real time to critical incidents that can affect their network infrastructure. A delay in responding to critical incidents can lead to a major security catastrophe. Most SIEM solutions come with built-in alert profiles and the option to customize and create new alert profiles.</p>	<p>The EventLog Analyzer SIEM allows administrators to configure and set real-time alerts from a huge list of out-of-the-box alerts. It also has the flexibility to customize and configure alerts based on threshold conditions, event IDs, log message, etc. IT administrators are notified in real time via email and SMS when any anomalous activity or threshold violations happen on the network. The EventLog Analyzer SIEM also allows you to execute custom scripts or programs upon alert generation to take quick remedial action for securing your network.</p>

Object Access Auditing


EventLog Analyzer SIEM Advantage


Most administrators face the challenge of detecting what actually happened to their files and folders – who accessed them, deleted them, edited them, moved them, etc. Object access auditing capability can help administrators meet this challenge head-on. With object access auditing, organizations can secure their business-critical data, such as employee data, accounting records, intellectual property, patient data, financial data, etc.


One of the key goals of object access audits is regulatory compliance. Regulatory compliance bodies such as Sarbanes Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Payment Card Industry (PCI) require organizations to adhere to a set of rules related to data security and privacy. Unauthorized access, accidental access, files/folders deletion, changes in files/folders, or permissions open the door for data thefts and can lead to a non-compliant status for the organization. This can be quite costly and also tarnish your company's brand value.


Using the EventLog Analyzer SIEM, you can collect all your object access audit logs at a centralized location and manage the object access audit logs effectively. You can now track all success and failure access attempts on folders and files in your enterprise. EventLog Analyzer sends alerts via SMS or email in real time when your sensitive files/folders are accessed by unauthorized users.

With the EventLog Analyzer SIEM, you get precise information of object access such as which user performed the action, what was the result of the action, on which server it happened, and the user workstation/network device from where the action was triggered.

 User Monitoring	EventLog Analyzer SIEM Advantage
<p>Most major data breaches have happened because organizations have failed to monitor the activities of their users, especially users who have privileged rights. SIEM solutions, with real-time user monitoring, help in detecting system and data misuse.</p> <p>To secure the network from breaches and threats due to user activities, organizations need to monitor user activity proactively in real time. This is also necessary to meet security compliance requirements such as PCI DSS, HIPAA, ISO 27001, SOX, etc.</p>	<p>The EventLog Analyzer SIEM monitors all users in real time and provides exhaustive reports with a complete audit trail of all user activities. It also generates privileged user monitoring and auditing (PUMA) reports by tracking the activity of privileged users.</p> <p>With the EventLog Analyzer SIEM, IT administrators get precise information in real time on critical events such as user logons, user logoffs, failed logons, successful audit logs cleared, audit policy changes, objects accessed, user account changes, etc.</p>

 File Integrity Monitoring	EventLog Analyzer SIEM Advantage
<p>File integrity monitoring (FIM) helps thwart data breaches and meet stringent compliance requirements observed by enterprises. When unauthorized or disgruntled users access and misuse confidential data, such as social security numbers, financial records, and other sensitive information of the enterprise, it can cause irreparable harm to a company and its stakeholders.</p> <p>Compliance acts such as the PCI DSS, SOX, HIPAA, and etc. have made it mandatory for companies to monitor in real time all changes that happen to their files and folders by using file integrity monitoring (FIM) automation solutions.</p>	<p>The EventLog Analyzer SIEM facilitates real-time file integrity monitoring (FIM) by protecting sensitive data, helping organizations meet their compliance needs.</p> <p>With the EventLog Analyzer SIEM's file integrity monitoring capability, security professionals can now centrally track all changes happening to their files and folders, such as when files and folders are created, accessed, viewed, deleted, modified, renamed, and much more. This critical information provided by the EventLog Analyzer SIEM helps users make quick decisions and mitigate the risk of data breaches.</p>

 Reporting	EventLog Analyzer SIEM Advantage
<p>IT administrators make decisions based on the security reports generated by their SIEM solution. The reports need to be precise and accurate. SIEM solutions provide several out-of-the-box security and compliance reports that can be generated within minutes and also be scheduled at a particular time/day.</p> <p>Security reports need to have a good design, and the data has to be well structured. Custom report builder helps administrators create security reports to meet their internal security requirements. The custom report builder in any SIEM solution needs to be flexible, allowing the IT administrator to add/remove specific security criteria when building the custom report.</p>	<p>The EventLog Analyzer SIEM includes several out-of-the-box security reports for your network systems, devices, and applications. These out-of-the-box reports present details of the top events generated, event trends, user activity, regulatory compliance, historical trend, and more.</p> <p>The EventLog Analyzer SIEM also provides the custom report building feature that allows IT administrators generate reports to meet their security requirements. The reports generated by the EventLog Analyzer SIEM are accurate, precise, and user-friendly, which can be easily interpreted even by a non-technical person.</p>

 Dashboards	EventLog Analyzer SIEM Advantage
<p>Dashboards drive SIEM solutions and help IT administrators take timely action and make the right decisions during network anomalies. Security data must be presented in a very intuitive and user-friendly manner. The dashboard must be fully customizable so that IT administrators can add and view only the security information they need.</p>	<p>The EventLog Analyzer SIEM dashboard is very intuitive and 100% customizable with the drag-and-drop capability. The EventLog Analyzer SIEM dashboard supports widgets that allow IT administrators to keep only relevant IT security information on their dashboard and not be confined to prefixed graphs and charts that may even be irrelevant to them. The security data is presented in easy-to-understand graphs and charts, wherein the IT administrator can also drill down the data shown and run a root cause analysis within minutes.</p>



System and Device Log Monitoring

Network systems and devices are the most important part of any IT infrastructure. The log data generated by your servers, workstations, routers, switches, etc. contain vital information that can be leveraged to mitigate network threats, such as prevent data thefts, detect network anomalies, and monitor user activities.

Manually analyzing the log data generated by your network systems and devices is quite difficult. Therefore, automating log monitoring and analyzing system and device logs in real time will help administrators reduce network downtime, increase network performance, and strengthen network security.

EventLog Analyzer SIEM Advantage

The EventLog Analyzer SIEM enables security professionals to monitor their network systems (servers, workstations, virtual machines, etc.) and devices (routers, switches, etc.) and get notifications in real time by SMS or email during anomalous or suspicious activity on network systems and devices.

Using the EventLog Analyzer SIEM, administrators can now analyze, monitor, report, search, and archive log data from network systems and devices at a centralized location.



Log Retention

Log retention or archiving is very important for organizations to meet various compliance regulatory requirements, such as SOX, HIPAA, PCI DSS, FISMA, and more. Archived log data is used for log forensic investigation, allowing IT security professionals to drill down the log data and do a root cause analysis to track down the network intruder and the event activity that caused the network problem.

EventLog Analyzer SIEM Advantage

The EventLog Analyzer SIEM retains all log data generated by network systems, devices, and applications in a centralized repository for any period of time. IT administrators can use the archived log data to meet compliance requirements, to conduct log forensic investigation, and during internal audits. The EventLog Analyzer SIEM encrypts the log archive files to ensure that the log data is secured for future forensic analysis and compliance/internal audits. The archived log data is further secured by hashing and time

Business Benefits of SIEM

The business benefits of deploying a SIEM solution in your enterprise include:

Rapid ROI

Managing log data manually is close to impossible due to the data volume. SIEM solutions make effective use of the log data and automate the entire process of log management (collection, analyzing, alerting, reporting, and more), enabling your IT administrators to provide top-notch IT security in a short span of time. With an SIEM solution in place, IT administrators will find time to invest more on strategic IT than in manually managing their log data.

Real-time Monitoring

Without real-time monitoring, it's impossible for IT administrators to determine what exactly is happening on their network. SIEM solutions facilitate real-time monitoring and provide powerful insights and network security intelligence into user behaviors, network anomalies, system downtime, policy violations, internal threats, regulatory compliance, etc.

Reporting

Generating multiple security reports can be tedious without a centralized reporting tool. SIEM solutions have the capability to store log data from network systems, devices, and applications at a central place, enabling IT administrators to generate various security reports with a click.

Cost Saving

Rather than using multiple point products to meet the IT security needs of the enterprise, SIEM solutions unite all critical IT security capabilities such as compliance reporting, file integrity monitoring, user monitoring, device monitoring, etc. Enterprises using SIEM solutions save huge amounts of money, which otherwise would have been spent in purchasing multiple security tools. Also, the maintenance cost associated with multiple log management and analysis point products is totally eradicated by having a single SIEM tool.

Stay Compliant

SIEM solutions help enterprises meet regulatory compliance requirements by monitoring and analyzing log data from their IT infrastructure in real time. SIEM solutions provide enterprises with out-of-the-box IT compliance reports such as PCI DSS, SOX, HIPAA, FISMA, ISO 27001, etc., allowing IT administrators to be ready with the relevant security reports to be produced to the auditor during the compliance audit.

Conclusion

Security threats to a company are always on the rise, and companies need to protect their network adequately. A SIEM solution can provide enormous security benefits to the company by protecting the network with real-time log analysis about data breaches and sophisticated cyber attacks.

Most organizations think that SIEM solutions have a steep learning curve and are expensive, complex, and hard to deploy. This claim may be true about many SIEM vendors. However, the right SIEM solution is one that can be easily deployed, is cost-effective, and meets all your IT security needs with a single tool.

About the Author



Joel John Fernandes currently works as a Senior Product Marketing Analyst for ManageEngine. He has thorough knowledge in the Security Information and Event Management (SIEM) and Payment Card Industry Data Security Standard (PCI DSS) domain and has consulted on network security and log management for both large and small enterprises. He can be reached at joeljohn.f@manageengine.com

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.

 <http://blogs.manageengine.com>

 www.facebook.com/manageengine

 <https://twitter.com/manageengine>



ManageEngine EventLog Analyzer

Advanced SIEM Solution

www.eventloganalyzer.com

Zoho Corporation

4141 Hacienda Drive
Pleasanton, CA 94588, USA

Phone: +1 888 204 3539

Website: www.manageengine.com

ManageEngine
Powering IT ahead