ManageEngine

# Why your Enterprise needs a Security Information and Event Management (SIEM) Solution?

**Joel John Fernandes**
Author and SIEM Expert

whitepaper

# Introduction

Security Information and Event Management (SIEM) solutions were introduced to provide enterprises with network security intelligence and real-time monitoring for network devices, systems and applications. With 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.

Network infrastructures of any enterprise include network devices (routers, switches, firewalls, etc.), systems (Windows, Linux, etc.) and business critical applications that generate a huge amount of log data. These log data contains vital information that 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 log data that is generated is enormous and not enough actionable information can be derived from it if done manually. Real-time log monitoring and analysis cannot be achieved if done manually. Automation is the key and that's where Security Information and Event Management (SIEM) solutions come in to automate the entire process of log management thereby providing real-time network security.

In this white paper, we'll discuss the challenges faced by IT administrators in managing terabytes of log data for IT security purposes. Plus we'll explore the 14 critical capabilities common to most SIEM solutions and how ManageEngine EventLog Analyzer SIEM solution can help enterprises in meeting their IT security needs effectively. Finally we'll highlight the business benefits an enterprise can gain when planning to deploy a SIEM solution.

# Network Security and Log Management Challenges

We'll now discuss some key network security and log management challenges faced by enterprises.

## Log Analysis

The task of analyzing precise information in real-time from terabytes of log data holds as the greatest challenge for network administrators. Analyzing and correlating log data manually for IT security is impossible and is always prone to human error. Administrators need to rely on automated solutions that can help them in analyzing the huge amounts of log data generated by their network infrastructure. Administrators need to be notified in real-time during anomalies in applications, systems, and devices. Analyzing log data using automated tools can also help administrators to identify suspicious user activities on the network.

## Log Collection

The process of 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 using agents or agentless mechanism. Using agents or not using them totally depends on the security policies charted by the organization. Having multiple tools to manage different log formats from numerous devices, systems and applications is always a pain and not an effective way to manage the logs in an enterprise. IT administrators need a single tool that allows them to decipher any log format from any source at a central place.

## Meeting IT Compliance Requirements

Every IT administrator wants the compliance auditors to finish their audit work effortlessly and make a move quickly. Verbally assuring the compliance auditors is not at all sufficient. Compliance reports have to be ready and all the reports have to be proved by showing the auditors the log data and the tools used to manage the logs generated by the network infrastructure. Meeting the 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. Enterprises are now proactively moving ahead to demonstrate compliance because having a secure IT network results in improved quality, competency, high brand value and customer satisfaction.

## Log Search

Conducting a search on logs to find the root cause of the 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 it the most. IT administrators need search capabilities that would allow them to conduct log forensics thereby allowing them to find and remediate their network issues and anomalous behavior quickly. Log search capabilities should give the network administrator the freedom to conduct a search across his network infrastructure.

## Data Representation

Network administrators need better data representation in different graphical formats, reports and dashboards. Viewing and analyzing log data in a graphical manner is a preferred choice rather than looking at raw log data. Instead of spending time sifting through raw log data and gaining intelligence, one glance at the graphical representation has to drive the administrator to make decisions. Dashboard is among the most critical components of an IT security solution. It is the primary interface to monitor real-time events and to perform analysis, reporting and manipulation of stored log data. Presenting the vital information from the log message in form of graphs and charts is very much essential to help administrators to take timely action.

## Track Suspicious Behavior

Data thefts, outages and system crashes can be caused by your most trusted employees and users having privileged access to business critical applications, devices, systems and files. Confidential data has been misused and has led to a hefty monetary loss 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 during anomalous activity happening on their network devices, applications, systems, files, etc.

## Centralized Log Archiving

One of the most challenging tasks in log management for enterprises is archiving logs. Archiving logs at a central place is a mandate for all enterprises to meet compliance requirements. Log archiving depends of the policies laid down by the enterprise and predominately by the regulatory compliance followed by them. The log archiving period varies for different compliance audits such as PCI DSS requires 1 year, HIPAA requires 7 years, FISMA requires 3 years, etc. Another good reason for archiving logs at a central place is for conducting log forensic investigation. Also, archived log data must be protected from changes for authenticity.

## Why SIEM?

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

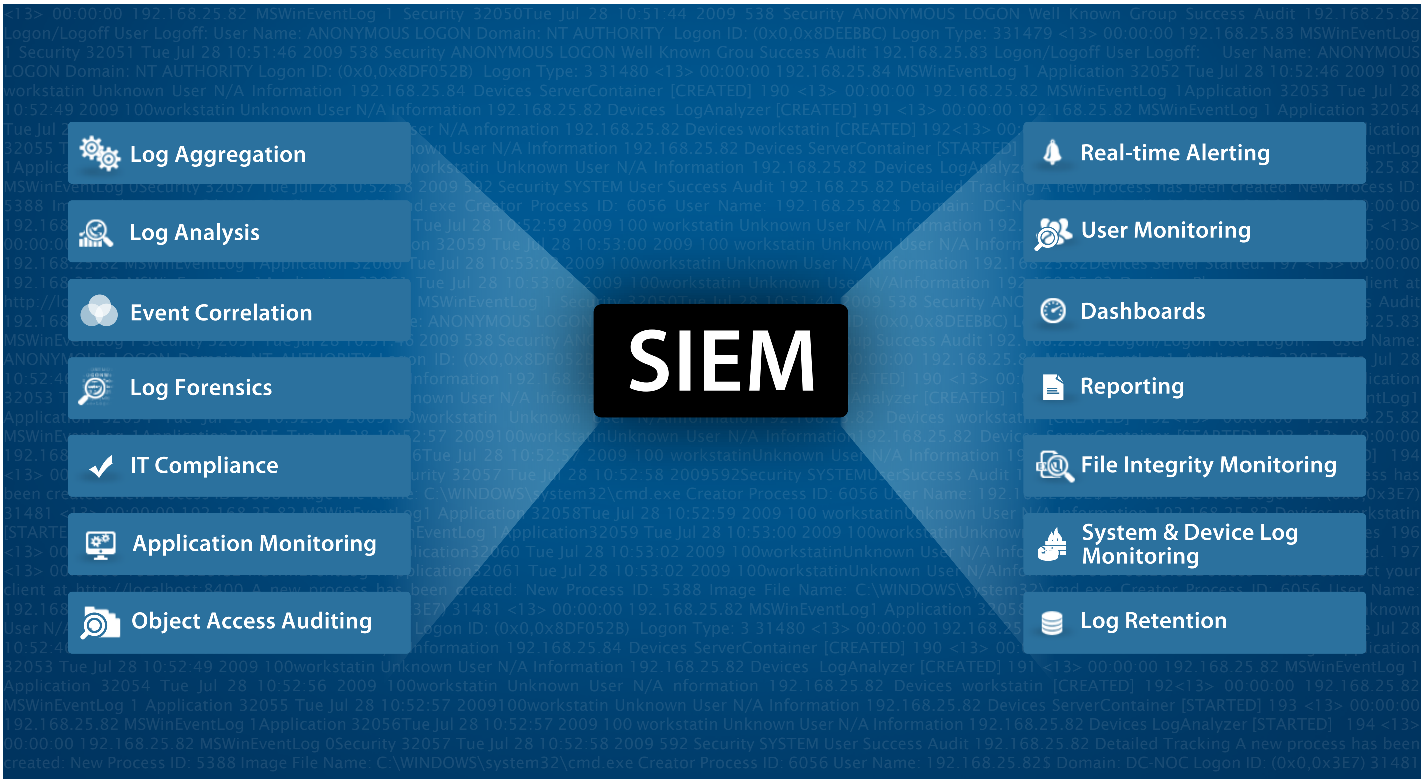
Organizations need to have tools that can derive meaningful, actionable information and security intelligence from the log data. Monitoring and analyzing log data is not a one-time process that will secure your network. It should be an ongoing process followed by the IT department where in the log data 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 bring automation in managing terabytes of log data for IT security purposes. SIEM solutions provide real-time monitoring of network systems, devices and applications by providing security intelligence to mitigate threats, identify the root causes of security incidents and to meet compliance requirements.

## SIEM Product Alert

## Critical Security Information and Event Management (SIEM) Capabilities

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



### Log Aggregation

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 place. Universal log collection is also a critical requirement for enterprises looking out to deploy a SIEM solution.

The advantage of SIEM solutions having universal log collection feature allows enterprises to aggregate and analyze any log data format from any source. Also, the log aggregation method should be kept into consideration – Agent based collection and Agentless collection. Using agents or not using them totally depends on the security policies followed by the organizations.

## Log Aggregation using EventLog Analyzer SIEM

EventLog Analyzer SIEM aggregates logs from heterogeneous sources (Windows systems, Unix/Linux systems, Applications, Databases, Routers, Switches, etc.) at a central place. EventLog Analyzer SIEM also supports universal log collection using its Universal Log Parsing and Indexing (ULPI) technology that allows you to decipher any log data regardless of the source & log format.

While most log data from the network infrastructure can be collected via agent-less method, EventLog Analyzer SIEM also offers agent technology to meet the diverse requirements of an enterprise.

## Log Analysis

Analyzing raw log data and generating intelligence for IT security in real-time forms the core of every 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 have the flexibility to easily drill down through log data shown on the dashboard to get more insights and conduct a root cause analysis within minutes.

## Log Analysis using EventLog Analyzer SIEM

EventLog Analyzer SIEM performs analysis on the log data collected from your network devices, systems and applications in real-time allowing IT administrators to mitigate threats and detect network anomalies proactively. The actionable security data is shown on the dashboard in form of graphs and charts. You can drill down on the data shown on the dashboard and perform a root cause analysis to identify the incident that caused the security activity.

IT administrators can also generate security reports at any given point in time due to real-time log analysis. The data shown on the dashboard and security reports can be easily customized as per the needs of the organization.

## Event Correlation

Real-time event correlation is all about proactively dealing with threats. Correlation of events allows network administrators to boost their network security by processing millions of events simultaneously in order to detect anomalous events happening on the network. 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 using log search scripts and alerts.

## Event Correlation using EventLog Analyzer SIEM

EventLog Analyzer SIEM provides a powerful correlation engine to proactively mitigate threats. It includes predefined correlation alerts based on threshold conditions or anomalous events which can be customized. The IT administrator gets notified in real-time during any threshold violations or network anomalies via SMS or Email.

Multi-event correlation can be done using the advanced log search feature provided by EventLog Analyzer SIEM wherein the IT security professional can do a root cause analysis by correlating multiple events and attributes.

## Log Forensics

SIEM solutions help security professionals to conduct log forensics investigation by allowing them to conduct a root cause analysis to track down the network intruder or the event activity that caused the network problem. The log forensics process should be very intuitive and user friendly thereby allowing IT administrators to search the raw log data with ease. Log search queries once entered by the IT administrator should quickly pinpoint the exact log entry which caused the security activity, find the exact time at which the corresponding security event had happened, who initiated the activity and also, the location from where the activity originated.

## Log Forensics using EventLog Analyzer SIEM

EventLog Analyzer SIEM makes forensic investigation very easy with its powerful log search functionality and instantly generates forensic reports based on the search results. EventLog Analyzer SIEM provides two different log search capabilities; the Basic Search and the Advanced Search. Both search capabilities provide powerful log search capabilities for your log data.

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 when using basic search. EventLog Analyzer SIEM's advanced search has much more sophisticated search capabilities but the ease of use remains the same like basic search.

## IT Compliance

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

Organizations who have to meet compliance requirements need to monitor their network in real-time, ensure high levels of security for their confidential enterprise assets and provide network audit reports to auditors when demanded.

### IT Compliance using EventLog Analyzer SIEM

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.

EventLog Analyzer SIEM also provides a value added feature to customize existing compliance reports. It also allows IT administrators to generate new compliance reports to help comply with the growing new regulatory acts demanding compliance in future.

## Application Monitoring

IT administrators need to effectively monitor the logs of their business applications such as databases, DHCP servers, Web servers, etc. Network hackers can easily gain access to your business applications and cause a data breach if your 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 happening on their network applications.

### Application Monitoring using EventLog Analyzer SIEM

EventLog Analyzer SIEM allows IT administrators to monitor their business critical applications in real-time and proactively detects anomalies/suspicious activities happening on their applications. 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 reports, administrators can easily determine errant users, and abnormal behavior of applications, thereby reducing the troubleshooting cycle.

No log management solution vendor will provide out-of-box log collection and reporting functionality for your custom in-house/proprietary applications. EventLog Analyzer SIEM using its Universal Log Parsing and Indexing (ULPI) technology allows you to analyze and generate reports for any log data collected from your in-house/proprietary applications.

## Object Access Auditing

Most administrators face the challenge of knowing 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 to meet this challenge head-on.

Object access auditing is a critical requirement for organizations and helps network administrators to secure their enterprise network. 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 strict set of rules related to data security and privacy. Unauthorized access, accidental access, files/folders deletion, changes in files/folders, or permissions opens the door for data thefts and can result in getting your organization a non-compliant status which not only is a costly affair but will also tarnish your company's brand value.

### Object Access Auditing using EventLog Analyzer SIEM

Using EventLog Analyzer SIEM you can collect all your object access audit logs at a centralized location and manage your object access audit logs effectively. You can now track all success and failure access attempts on folders and files in your enterprise.

EventLog Analyzer provides object access reports in user friendly formats (PDF and CSV) and sends alerts when your sensitive files / folders are accessed by unauthorized people in real-time via sms or email. With 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 tracks down the user workstation/network device from where the action was triggered.

## Real-time Alerting

Real-time alerting is a mandate for every SIEM solution and should alert IT security professionals when network anomalies and suspicious activities occur on the network.

IT administrators need to monitor, detect and respond to critical incidents that can affect their network infrastructure in real-time. A delay in responding to critical incidents can end up causing a major security catastrophe. Most SIEM solutions come with built-in alert profiles and also provide the option to customize and create new alert profiles.

### Real-time Alerting using EventLog Analyzer SIEM

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. EventLog Analyzer SIEM also allows you to execute custom scripts or program upon alert generation to take quick remedial action for securing your network.

## User Monitoring

Most major data breaches have happened because organizations have failed to monitor the activities of their users, especially users having privileged rights. SIEM solutions with real-time user monitoring helps in detecting system and data misuse.

To secure your network from breaches and threats that can rise due to user activities, organizations need to take proactive measures to ensure the activity of their users is monitored in real-time. Another major reason for enterprises to monitor their users is to satisfy security compliance requirements such as PCI DSS, HIPAA, ISO 27001, SOX, etc.

### User Monitoring using EventLog Analyzer SIEM

EventLog Analyzer SIEM monitors all users in real-time and provides exhaustive reports with a complete audit trail of all the activities done by users. It also generates privileged user monitoring and auditing (PUMA) reports by tracking down the activity of privileged users.

With 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. Administrators are notified via SMS or email in real-time when there is any suspicious user behavior happening on the network infrastructure.

## Dashboards

Dashboards drive SIEM solutions and help IT administrators to take timely action and make accurate decisions during network anomalies. Security data has to be presented in a very intuitive and user friendly manner. The dashboard has to be fully customizable allowing IT administrators to add and view only the security information that they need.

### Dashboards using EventLog Analyzer SIEM

EventLog Analyzer SIEM dashboard is very intuitive and 100% customizable with drag and drop capability. EventLog Analyzer SIEM dashboard supports widgets that allow IT administrators to keep relevant IT security information they want on their dashboard and not be confined with prefixed graphs and charts which are not relevant to them. The security data is presented in user friendly and easy to understand graphs and charts wherein the IT administrator can also drill down on the data shown in the graphs/charts and run a root cause analysis in minutes.

## Reporting

IT administrators make decisions based on the security reports generated by their SIEM solution. The reports generated by SIEM solutions need to be precise and accurate. Most 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.

Security professionals prefer security reports in PDF and CSV formats. The reports should have a good design and the data has to be well structured. Custom report builder helps administrators to create security reports to meet their internal security requirements. The custom report builder in any SIEM solution needs to be very flexible thereby allowing the IT administrator to add/remove specific security criteria’s when building the custom report.

## Reporting using EventLog Analyzer SIEM

EventLog Analyzer SIEM includes several out-of-the-box security reports for your network systems, devices and applications. These out-of-the-box reports show you details of the top events generated, event trends, user activity, regulatory compliance, historical trend and more. EventLog Analyzer SIEM also provides the custom report building feature that allows IT administrators to generate reports to meet their security requirements. The reports generated by EventLog Analyzer SIEM are accurate, precise and user friendly which can be easily interpreted even by a non-technical person.

Using these reports, administrators can easily determine suspicious users, meet internal security audit policies and comply with external regulatory bodies.

## File Integrity Monitoring

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 inflicts irreparable harm to a company and its stakeholders.

Compliance acts such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA) and other regulatory mandates have made it mandatory for companies to monitor all changes that happen to their files and folders in real time using file integrity monitoring (FIM) automation solutions.

## File Integrity Monitoring using EventLog Analyzer SIEM

EventLog Analyzer SIEM facilitates real time file integrity monitoring (FIM) by protecting sensitive data thereby allowing organizations to fulfill their compliance needs.

With 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 EventLog Analyzer SIEM allows users to make quick decisions and mitigate the risk of data breaches.

## 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 - prevent data thefts, detect network anomalies and monitor user activities.

Manually analyzing the log data generated by your network systems and devices is impossible. Automating log monitoring and analyzing the system and device logs in real-time will help administrators to reduce network downtime, increase network performance and strengthen network security.

### System and Device Log monitoring using EventLog Analyzer SIEM

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

With 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 in order to meet compliance regulatory requirements such as SOX, HIPAA, PCI DSS, FISMA, etc. Archived log data is used for log forensics investigation thereby allowing the IT security professionals to drill down into the log data and do a root cause analysis to track down the network intruder and the event activity that caused the network problem.

### Log Retention using EventLog Analyzer SIEM

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

## Business Benefits of SIEM

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

### Rapid ROI

SIEM solutions make effective use of the log data generated by your network infrastructure, thereby allowing IT administrators to provide top notch security for their network in a short span of time.

### 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 a painful task without a centralized reporting tool. SIEM solutions have the capability of collecting log data from network systems, devices and applications at a central place thereby allowing IT administrators to generate a wide range of security reports by reducing the report generation process from days to couple of hours.

### 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. in a single SIEM solution. Enterprises using SIEM solutions save huge amounts of money which otherwise would have been spent purchasing multiple security tools. Also, maintenance costs associated with multiple log management and analysis point products are totally eradicated by having a single SIEM tool.

### Stay Compliant

SIEM solutions help enterprises to 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. thereby allowing the IT administrators to be ready with the relevant security reports to be produced to the auditor confidently during the compliance audit.

# Conclusion

The security threats to a company are always on a rise and enterprises need to protect their network from falling into wrong hands.  A SIEM solution can provide enormous benefits to the enterprise if used correctly with specific requirements in mind.

Most organizations think that SIEM solutions have a high learning curve and are expensive, complex, and hard to deploy. The above claim holds true with many SIEM vendors but the most important thing is selecting the right SIEM solution that can be easily deployed, cost-effective and can get you up and running in couple of hours.

Finally if you are planning to invest in a SIEM solution, evaluate ManageEngine EventLog Analyzer SIEM. It's the most cost-effective and powerful SIEM solution available in the market.

### 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) domain and has consulted both large and small enterprises on issues of network security and log management. 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