

USE CASE

Securing resources and data on the cloud



Securing resources and data on the cloud

Businesses are increasingly moving to the cloud for advantages such as scalability, agility, and zero-risk failure, all of which are more challenging in on-premises environments. While cloud platforms like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure ensure the security of the cloud, it's the organization's responsibility to secure data stored on the cloud. This calls for a security information and event management (SIEM) solution, which can offer cloud support with features such as constant and centralized monitoring of all devices, applications, users, and other cloud infrastructure components.

How Log360 helps

ManageEngine Log360, an easy-to-use SIEM solution, offers support for cloud services. Log360's cloud monitoring component provides comprehensive reports, easy search mechanisms, and customizable alert profiles that facilitate the smooth functioning of your business by:

Extensively auditing cloud environments:

Log360 currently supports AWS, Azure, Google, and Salesforce cloud platforms. Log360 provides a central dashboard with detailed information on what's happening on every cloud platform. With numerous security dashboards that are updated in real time, you can get vital information on a wide variety of actions from user activity to database changes.

Monitoring dynamic cloud configuration changes in real time:

Cloud workloads are highly dynamic, where systems can be added and removed in seconds. Log360 provides multiple security dashboards to monitor these configuration changes with information on virtual machines, auto-scaling, template changes, snapshot changes, group changes, and much more across various cloud platforms. Log360 can also help you set up threshold-based alerts to notify you of configuration changes made by unauthorized persons in your cloud environment.

Spot anomalous user behavior in your cloud environment:

Cloud platforms often come with multiple management capabilities that make tracking every activity of the user tedious. This makes it easy for malicious insiders to remain inconspicuous. Log360 has a user and entity behavior analytics (UEBA) add-on that automatically spots anomalous user behaviors using machine-learning algorithms.

Detect unauthorized access in real time across cloud platforms:

Unauthorized access is deemed the biggest threat to cloud security. Unauthorized access occurs through misuse of employee credentials and improper access controls. Log360 monitors all user activity, permission changes, file accesses, file changes, database changes, content activity, and much more across the supported cloud platforms. You can detect unauthorized access in real time with built-in alerting. With extensive access monitoring and real-time alerts, ensure adherence to data security regulations.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a
Customers' Choice for SIEM

[Check out why](#)

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in
Gartner's Magic Quadrant for
Security Information and Event
Management, 2020.

[Get the report](#)

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine
Log360[\\$ Get Quote](#)[↓ Download](#)