ManageEngine

Log360
vs.
Log360 MSSP

What sets them apart?

ManageEngine Log360

ManageEngine Log360 is a SIEM solution designed to help enterprises monitor and respond to diverse log data across their IT infrastructure. The solution excels in centralizing logs from different network entities, providing real-time security event analysis and facilitating compliance management.

ManageEngine Log360 MSSP

Log360 MSSP (on-premise) is a unified SIEM that can help you collect, analyze, manage, and search through the log data of clients across different geographic regions. With a centralized client management console, client specific dashboards, and dedicated technician assignment and management, the solution makes it easier to manage multiple client environment without much hassle.

Shared features in
Log360 and Log360 MSSP

Security analytics

Experience real-time, comprehensive insights into your network security through dynamically updated graphical dashboards. Gain full visibility into your IT landscape from any location using multiple security dashboards, ensuring a detailed overview of your network's security posture.

Compliance

Both editions feature an integrated compliance management console designed to help an organization fulfill regulatory mandates. This ensures adherence to compliance requirements outlined in standards such as PCI DSS, FISMA, GDPR, SOX, HIPAA, and ISO 27001.

Rule-based correlation

The correlation engine empowers you to create rule-based alerts for known threats, receive notifications for malicious activities, and view chronological event sequences for potential threats.

Incident response

Both share robust incident response capabilities aimed at swiftly identifying and mitigating security threats. Upon detection, both solutions provide customizable alerting and notification features, promptly notifying designated personnel or stakeholders.

AD auditing

AD auditing enables real-time monitoring and reporting of granular changes to AD objects, tracks user logon activities, monitors alterations to various AD entities, guards against privilege abuse, and extends threat detection by correlating AD actions with other network events.

Choosing between
Log360 and Log360 MSSP

For organizations with varying operational requirements, the choice between Log360 and Log360 MSSP hinges on the deployment type.

Feature	Log360	Log360 MSSP
Tenancy requirements	Tailored for managing a single client, Log360 ensures dedicated attention to individual data privacy and security measures.	Ideal for those managing multiple customer profiles, the MSSP edition streamlines processes through a centralized console, ensuring logical separation of each customer's data for stringent data privacy and security.
Client-specific dashboard	Log360 offers a real-time, comprehensive perspective of your network's security through a variety of auto-updated graphical dashboards.	For organizations requiring personalized client dashboards, Log360 MSSP accommodates their unique preferences and needs, enhancing the overall client-centric security management experience.
Dedicated technician management	In Log360, role assignments are possible within the SOC team, encompassing administrator, operator, and guest roles for App Account assignments, and administrator and user roles for organization assignments. Each role carries distinct privileges and responsibilities.	Choose Log360 MSSP when dedicated technician assignment and management are essential. The MSSP edition provides role-based access control (RBAC), allowing efficient assignment of technicians to specific clients. This ensures data privacy and enhances operational effectiveness.
Licensing	Log360 comes in a single edition viz., Standard Edition. Licensing is based on the number of devices being monitored.	Log360 MSSP has "Manage Client License" section, used to allocate components and view allocated components for each client. This section can also be used to view the license status of each client and its child components.