ManageEngine
Log360 Cloud

Cloud SIEM and auditing made easy with Log360 Cloud

Protect your digital business from ever-evolving cyberthreats by deploying ManageEngine Log360 Cloud, a security information and event management (SIEM) solution for your cloud infrastructure.

Log360 Cloud, with built-in cloud access security broker (CASB) capabilities, aids in the collection, storage, and management of network logs, and helps IT security teams achieve their security and compliance objectives.

Take your cloud security operations to the next level with Log360 Cloud

Protect your digital business from ever-evolving cyberthreats by deploying ManageEngine Log360 Cloud, a SIEM solution for your cloud infrastructure.Log360 Cloud seamlessly addresses your log management and compliance needs by collecting logs from both on-premises and cloud-based data sources, storing those logs in the cloud, and providing a comprehensive view of your network's security in real time with multiple dashboards. With Log360 Cloud, you can:

Get the benefits of a SIEM solution, but in the cloud.

- Reduce your log storage spending
- Avoid shadow IT by tracking unsanctioned app usage
- Collect logs from both on-premises and cloud environments
- Scale your network architecture

Trusted by some of the leading businesses globally

UNISYS · accenture · IBM · NSE · SIEMENS · Infosys · EY · LANB

Deloitte. · tcs TATA CONSULTANCY SERVICES · xerox · nielsen · ebay · MICHIGAN STATE UNIVERSITY · TOYOTA · Panasonic

Utilize rule-based attack detection and threat intelligence

Log360 Cloud enables you to create rule-based alerts for known attacks, indicators of compromise (IoC), and more, with the built-in correlation module. The threat intelligence and advanced threat analytics capabilities of Log360 Cloud automatically update threat data from trusted open-source threat feeds, and notify you when a malicious source tries to interact with your IT environment.

Comply with regulatory mandates

Log360 Cloud meets IT compliance requirements to ensure data privacy and security. The solution helps your organization monitor and meet regulatory mandates, like PCI-DSS, FISMA, GLBA, SOX, HIPAA, and ISO 27001, by leveraging audit-ready report templates. It also provides dashboards and alerts specific to different regulations.

Gain visibility into dark web breaches

Log360 Cloud, through our integration with Constella Intelligence, facilitates dark web monitoring so you can proactively mitigate threats before attackers exploit leaked credentials, sensitive personal and financial information on the dark web.

Machine-learning based anomaly detection with UEBA

Log360 Cloud’s user and entity behavior analytics uses machine learning to detect deviations from normal user and entity behavior. By identifying anomalies, assigning risk scores, and enabling custom anomaly rules, UEBA empowers your SOC to uncover insider threats, compromised accounts, and suspicious patterns that traditional methods may miss.

Reengineered threat detection

Log360 Cloud's reengineered detection console unifies correlation logic, MITRE ATT&CK® mapping, threat intelligence, UEBA insights, and provides 2000+ prebuilt cloud delivered detections in a single interface. Precision rule filters allow targeting of specific users, groups, or organizational units, which helps reduce alert fatigue and improve alert accuracy.

Monitor cloud applications with CASB

Log360 Cloud's built-in CASB lets you track cloud app and unsanctioned app usage, gain insights on users and applications, and ban malicious applications. Log360 Cloud also helps you monitor and control the use of shadow IT.

Speed up threat investigation with incident workbench

Log360 Cloud's incident workbench provides streamlined incident management. It offers consolidated analytics on crucial entities, an intuitive interface with advanced process hunting capabilities, integration with advanced threat analytics, and a centralized investigation console. This ensures quicker and more impactful investigations, enabling security teams to tackle security threats efficiently.

Security platform

Log360 Cloud Offers open API compatibility to ensure comprehensive data ingestion, analysis, and threat detection without missing critical security events. It Utilizes robust APIs and SDKs to build custom integrations, specialized extensions, and applications that can take its capabilities a step further. You can leverage predefined extensions or build your own to tailor Log360 Cloud’s functionality to your unique security environment.

AI-powered security investigation with Zia Insights

Log360 Cloud now includes Zia Insights, a contextual AI engine that transforms alert triage and incident analysis. Built on Azure OpenAI with BYOK support, Zia provides natural language summaries, visual timelines, MITRE ATT&CK® mapping, and remediation suggestions, helping SOC teams cut investigation time and act with clarity.

Scan the QR code to sign up.