ManageEngine
Log360

DATASHEET

Log360 for compliance

Log360, a comprehensive security information and event management (SIEM) solution, enables you to combine log management with compliance management, and helps organizations meet various auditing, security, and compliance needs.

Compliance management features

• Audit-ready report templates for compliance audits

Generate compliance reports from predefined templates for a wide range of policies, including PCI DSS, SOX, HIPAA, FISMA, GLBA, ISO 27001, and the GDPR. Fetch these reports with a single click, and export them as required.

• Custom compliance reports

New regulations can be issued at any time, so it's important to be prepared. Construct custom compliance reports for both new regulations and internal requirements with just a few clicks.

• Secure log archival

Most compliance policies require you to archive logs securely for a specified, minimum period of time, as they may come in handy in the forensic analysis of a data breach. Archive logs automatically at custom intervals with flexible archiving options, and store them in an encrypted form for as long as needed.

• Establishment of security controls

Certain regulations require you to have stringent security controls in place to help you detect security incidents early, and also prove that you have taken all necessary steps to secure your network from attacks. Build efficient security controls to meet compliance requirements with capabilities like incident detection mechanisms, data discovery, forensic reports, and incident management.

• Export reports easily

You can export reports from predefined and custom templates to PDF or CSV to provide to auditors. Also, schedule reports to be automatically generated and exported at predefined time intervals.

Other highlights of Log360

- Extensive auditing and alerting capabilities help you quickly detect and thwart threats.
- A powerful search engine, which helps you backtrack events so you can pinpoint the cause of the security incident, and extract crucial data to file an incident report.
- Automatically discovers Windows and Linux/Unix devices, network devices, SQL servers, and Microsoft Internet Information Services (IIS) web servers in your network.
- A real-time event response system to act on critical security events promptly.
- Alert profiles with email and SMS notifications.
- A real-time correlation engine to accurately identify defined attack patterns.

- User and entity behavior analytics (UEBA) to analyze logs from different sources to detect any deviation from normal behavior. Besides detecting anomalies, it also offers actionable insights to the IT administrator with the use of risk scores, anomaly trends, and intuitive reports.

- Cloud security capabilities to efficiently monitor, report on, and audit your public cloud infrastructure.

Supported log sources

Log360 supports log analysis and parsing of over 750 log sources. It also includes a custom log parser to analyze any human-readable log format. Some of the common log sources supported are mentioned below.

Applications
SQL and Oracle databases, IIS and Apache web servers, and more.

File servers
Windows, NetApp filers, EMC file servers, and file server clusters.

Network perimeter devices
Routers, switches, firewalls, IDS/IPS, and more.

Virtual platforms
Microsoft Hyper-V and VMware.

Cloud platforms
Azure, Amazon Web Services (AWS), Salesforce, Office 365, and Exchange Online.

Linux/Unix servers and devices

Windows servers and workstations

System requirements

Hardware requirements

Log360's on-premises deployment requires a dedicated server with the following hardware configuration:

Hardware	Minimum	Recommended
Processor	2.4Ghz	3Ghz
Core	Dual core	8 core
RAM	8GB	16GB
Disk space	60GB	150GB

Software requirements

ManageEngine Log360 supports the following Microsoft Windows operating system versions:

- Windows 2003
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2016
- Windows Server 2019

Supported browsers

ManageEngine Log360 requires one of the following browsers to be installed on the system to access the Log360 web client:

- Internet Explorer 9 and above
- Firefox 4 and above
- Chrome 10 and above
- Safari 5 and above