ManageEngine
Log360

DATASHEET

Data security with Log360

The consequences of a data breach can be devastating, and can put any organization out of their business quickly. Moreover, these breaches can leak your intellectual property and confidential information, while inviting huge penalties for breaking compliance requirements. Therefore data security becomes crucial for the wellbeing of your business.

Log360, the one-stop SIEM solution can help secure your sensitive data and ensure integrity with its abilities to:

Discover data

Find, analyze, and track sensitive personal data—also known as personally identifiable information (PII)—stored in files, folders, or shares.

Audit file servers

Monitor, report on, and receive real-time alerts for changes made to files and folders in your Windows file servers. Improve data security and information management in your Windows file server environment while meeting compliance requirements effectively.

Use machine-learning-powered UEBA to mitigate threats

Become proactive in your approach by identifying anomalous activity in your network. User entity and behavior analytics (UEBA) works by baselining user and entity behavior such as data access patterns, comparing it with past activities, and raising an alarm if this behavior deviates from normal patterns.

Detect modification of data

Protects your organization's data from unauthorized and unwanted modification and leaks. Log360's file integrity monitoring (FIM) module tracks any changes made to files and folders in real time to detect security incidents and notify security admins who can respond to them quickly.

Detect data leaks

Detect and respond to sensitive data leaks via USB devices, printers, emails, and more through real-time security monitoring. Log360's event correlation engine analyzes numerous events, adds business context to the analyzed events, and draws connections between them in a sequential manner before providing logical solutions to detected threats.

Other highlights of Log360

- Extensive auditing and alerting capabilities to help you quickly detect and thwart threats.
- Compliance management capabilities to help organizations meet their varied auditing, security, and compliance needs.
- Powerful search engine to help you backtrack so you can pinpoint the security incident and extract crucial data to file an incident report.
- Automatic discovery of Windows and Linux/Unix devices, network devices, SQL servers, and IIS web servers to reduce time and efforts of setting-up the solution.
- Real-time event response system to help you respond to critical security events promptly.

- Alerts feature to send out email and SMS notifications on security incidents based on configured alert profiles.
- Real-time correlation engine to help you identify the defined attack patterns accurately.

Supported log sources

Log360 supports log analysis and parsing from over 750 log sources. The tool also includes a custom log parser to analyze any human-readable log format. Some of the widely used log sources 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, AWS, Salesforce, Office 365, and Exchange Online.

Linux/Unix servers and devices

Windows servers and workstations

System Requirements

Hardware requirements

Log360 on-premise deployment requires a dedicated server with the following hardware configuration.

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

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

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