ManageEngine
Log360

Datasheet

Log360 is a comprehensive SIEM solution that helps enterprises combat threats and mitigate attacks.

Be it on-premises, in the cloud, or in a hybrid environment, Log360 has you covered.

Highlights of Log360

- Deploys in a few hours and delivers insights within minutes of deployment.
- Automatically discovers Windows and Linux/Unix devices, network devices, SQL servers, and IIS web servers in your network.
- Supports multiple environments, including physical environments, virtual platforms, and cloud platforms.
- Contains a unified console for auditing security events, securing confidential data, detecting potential threats, containing attacks, tracking incidents, and keeping your enterprise audit-ready.
- Reduces the burden on security operations centers (SOCs) with predefined alert profiles, reports, and correlation rules.

Core features

Security analytics

- Log 360 spots network threats by analyzing events from network devices, file servers, databases, web servers, Office 365, Exchange servers, and Active Directory.
- Instantly detects intrusions and issues alerts; contains intuitive dashboards and built-in reports.

Threat intelligence

- Quickly identifies external threats with its built-in, global IP threat database and STIX/TAXII threat feed processor.
- Helps identify and resolve security incidents quickly through an integrated alerting and incident management system.

Cloud monitoring

- Monitors widely-used public cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, and Salesforce.
- Helps you track, analyze, and react to events with comprehensive reports, an easy search mechanism, and customizable alert profiles.

User and entity behavior analytics

- Identifies anomalies, assigns risk scores to users and entities, and corroborates threats using machine learning.
- By recognizing subtle shifts in user activity, Log 360 detects internal threats, such as data exfiltration and user account compromises.

Data security

- Automatically discovers and protects personally identifiable information in Windows infrastructures.
- Monitors file and folder creation, deletion, modification, and permission changes in Windows file servers, NetApp file servers, EMC file servers and more.

Incident management

- Empowers you to immediately manage incidents with configurable, real-time alerts for threats.
- Integrates with help desk tools, such as BMC Remedy Service Desk, Jira Service Desk, Kayako, ServiceDesk Plus, ServiceNow, and Zendesk.

Integrated compliance management

- Offers predefined report templates that help comply with PCI DSS, GDPR, FISMA, HIPAA, SOX, and GLBA mandates.
- Lets you build your own compliance reports by customizing existing templates to meet internal security policies.

Supported event sources

Log360 supports log analysis and parsing for over 700 event sources. The tool also includes a custom log parser to analyze any human-readable log format.

Applications

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

Cloud platforms

Azure, AWS, Salesforce, Office 365, and Exchange Online.

File servers

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

Network perimeter devices

Routers, switches, firewalls, and IDS/IPS.

Virtual platforms

Microsoft Hyper-V and VMware.

Linux/Unix servers and devices

Windows servers and workstations

Specifications

Processor:
Any multi-core processor with a minimum of two cores.

RAM: 4GB

Disk Space Required: 40GB

Supported operating systems for installation

- Windows Server 2003 and above
- Windows Vista and above

Supported browsers

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

Supported databases

PostgreSQL and Microsoft SQL Server

Contact us:

Website: www.manageengine.com/log-management

Live demo: http://log360demo.manageengine.com

Sales questions: sales@manageengine.com

Tech support: log360-support@manageengine.com

Toll-free: +1-925-924-9500