GARTNER
2022

Placed in the **Gartner Magic Quadrant** for SIEM six consecutive times!

Get in touch with us!

Visit our website:
https://www.manageengine.com/log-management/

Support email:
log360-support@manageengine.com

Direct inward dialing:
+1.408.352.9254 +1.408.352.9254

Toll-free numbers:
US: +1.844.649.7766
UK: 0800.028.6590
AUS: 1800.631.268
CN: +86.400.660.8680
Intl.: +1.925.924.9500

Request a demo:

Why businesses **choose Log360**

> Log360 has made my job a cinch. The real-time reports and alerts make sure I don't have to spend a lot of time worrying about threats.

Victor,
IT security admin of SHM, London

> Log360 is a complete solution for all of the needs in events auditing! Subcomponents like EventLog Analyzer and ADAuditPlus are really helpful during reviews and audits.

Arvind Kumar,
IT security in charge, HCL Technologies, Noida

ManageEngine
Log360

Unified **SIEM solution** with **integrated DLP** and **CASB** capabilities

www.manageengine.com/fr/log-management

Experience cybersecurity like never before.

5 Reasons to choose **Log360**

Single console for cybersecurity:

A comprehensive solution that brings log management, Active Directory reporting, user behavior monitoring, data loss prevention, cloud security, and IT compliance management to a single console.

Analyzes almost any kind of data:

Supports over 700 types of log sources.
With the Custom Log Parser, automatically extract meaningful information from any human-readable log format.

Simple, unified SIEM:

Setting up Log360 is quick and easy. This intuitive SIEM solution takes less than a week to deploy, configure, and complete training.

Technical support for maximum value:

Hear our customers say it on Gartner Peer Insights! Our support team goes above and beyond to help you get the most out of Log360.

Affordable, best-in-class SIEM solution:

A flexible pay-for-what-you-use licensing model. Pick and pay for only the components that align with your security goals.

Log management

- **Intuitive security dashboards** display information in the form of graphs and reports, which help with discovering attacks, spotting suspicious user behaviors, and stopping potential threats.
- **Collect logs using both agent-based and agentless log collection options** from over 750 log sources and parse any log in human readable format with the built-in Custom Log Parser.
- **Analyze logs in depth and get actionable insights** through interactive dashboards displaying information in the form of graphs and intuitive reports.

Threat detection and modeling

- **The powerful correlation engine** includes over 30 predefined rules to detect known attacks such as SQL injection, denial-of-service, and firewall attacks.
- **Threat intelligence updates** from trusted third-party sources are used to detect APTs and meet compliance regulations.
- **User entity and behavioral analytics** can baseline normal user behavior and spot anomalies to effectively identify APTs.
- **Support for the MITRE-ATT&CK threat modeling framework** combined with security analytics helps with detecting sophisticated attack techniques.

Data loss prevention and security

- **Leverage data discovery and activity tracking** for sensitive data including personally identifiable information, Social Security numbers, and credit card numbers in file servers and storage.
- **Monitor file integrity** to track every access, creation, deletion, modification, and permission change made to critical files and folders.
- **Get real-time alerts** via SMS and email when unauthorized actions or anomalies are detected.

Security and risk posture management

- **Maintain your AD security posture** with the built-in security and risk management feature based on Microsoft's security baselines.
- **Continuously assess your AD environment** for risks and get recommendations for how to fix them.

Incident response and resolution

- **Automate your incident response** with built-in workflows that can be associated with incidents.
- **Carry out high-speed log forensics** to conduct post-attack analysis, identify attack patterns, and analyze the impact of security incidents.
- **Use the built-in incident ticketing tool** for process tracking, and integrate with third-party ticketing tools.

Integrated compliance management

- **Leverage audit-ready reports** for an exhaustive list of regulatory mandates including HIPAA, PCI DSS, GLBA, FISMA, ISO 27001, SOX, the GDPR, and much more.
- **Monitor compliance in real time** with dashboards for every regulation and real-time compliance alerts.
- **Use the custom compliance rule builder** with its simple drag-and-drop interface to conduct internal audits.

CASB implementation

- **Gain comprehensive visibility** into your AWS, Azure, Salesforce, and Google Cloud Platform cloud infrastructures.
- **Detect shadow** IT by monitoring unsanctioned cloud applications accessed by users.
- **Ensure cloud data security** by monitoring changes to users, network security groups, virtual private cloud, permissions, and more that occur in your cloud environment in real time.
- **Detect anomalous behavior** in cloud environments with machine-learning-based behavior analytics.

Vigil IQ

- **Harness the capabilities of Vigil IQ,** an advanced threat detection, investigation, and response (TDIR) system within Log360.
- **This powerful engine offers instant insights** into security threats through real-time correlation and adaptive alerts driven by machine learning.
- **High coverage to key security threats**, intuitive analytics, and automated playbooks help improve the mean time to detect (MTTD) and Mean time to respond (MTTR) facilitating timely action.

ManageEngine
Log360

Product **highlights**

Gain in-depth threat hunting through rule-based attack detection, forensic analysis, and support for the MITRE ATT&CK threat modeling framework.

Leverage user and entity behavior analytics to identify sophisticated threats and APTs.

Protect confidential data with the DLP module's sensitive data discovery, user activity tracking, unauthorized data access alerts, and data exfiltration alerts.

Expedite threat detection with in-depth threat hunting and actionable threat intelligence updates.

Secure your cloud infrastructure with deeper visibility into shadow IT, policy violations, content-aware data protection, and other CASB capabilities

Achieve security orchestration and automated response for your SOC using real-time alerts and workflows.