

AWARDS AND RECOGNITIONS



Placed in the **Gartner Magic Quadrant**
for SIEM

FORRESTER

2024

KUPPINGERCOLE
ANALYSTS

2024

GIGAOM

2024

Get in touch with us!

Visit our website:
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

“

With Log360's optimized detection rules and filtering techniques, we have reduced false or low-priority alerts by 90%, allowing our analysts to focus on the threats that matter most.

Corey Nelson,
IT manager, ECSO 911

“

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



Unified SIEM solution with integrated DLP, CASB, and Native SOAR capabilities

www.manageengine.com/log-management

Experience cybersecurity
like never before.

6 Reasons to choose Log360

Extensive detections

2,000+ prebuilt, cloud-delivered detection rules covering identity, endpoint, network, and cloud attack techniques.

Zia AI capabilities

Let Zia Insights turn alerts and incidents into clear summaries with entities, MITRE ATT&CK context, and next steps, while autonomous investigations uncover attack paths and accelerate response.

Built for scale

Enhanced scalability for high-volume log ingestion and correlation without slowdown.

Powerful rule-building

Flexible query grammar that lets you define precise rule criteria, use operators and functions, and craft advanced detection logic for custom security rules.

Native SOAR

Automate investigation, response, and remediation with native low-code orchestration engine and prebuilt playbooks.

Marketplace support

Extend Log360 with integrations such as CrowdStrike, Bitdefender, Cisco Duo, Okta, and Veeam for enhanced security operations.



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.



Threat detection and modeling

- The reengineered detection console combines correlation logic, MITRE ATT&CK® mapping, threat intelligence, UEBA insights, and rule-based alerting within a single interface. Detection content is continuously updated through the cloud to provide coverage for known threats, anomalous activity, and advanced attack patterns.
- Precision rule filtering options enable precise scoping of detections to specific users, groups, or organizational units, which helps eliminate noise and improve alert relevance. Multiple detection modes and tuning insights support the creation of refined rules that help reduce false positives.
- Threat intelligence updates from trusted third-party sources are used to detect APTs and meet compliance regulations.



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.



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.



Native SOAR and Security Automation

- Transform incident response operations with native SOAR capabilities powered by a built-in orchestration engine.
- Access 60+ ready-to-use playbooks and a visual drag-and-drop playbook builder.
- Orchestrate security operations across endpoint, identity, cloud, and IT systems from a single platform.



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.



AI-powered investigations

- Zia Insights transforms logs, alerts, and incidents into concise, easy-to-read summaries, highlighting key entities, mapping activity to MITRE ATT&CK techniques, and recommending next steps.
- Zia Alert Investigation Agent autonomously performs multi-step investigations on alerts to identify attacks, assess affected entities using risk and threat intelligence, build an attack timeline, and provide immediate mitigation guidance.



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.
- Constitutes a 3-way threat investigation workbench designed to achieve efficient and faster threat analysis and resolution



Dark web monitoring

- Monitor the dark web for any mention of your organization's sensitive information, including domain names, employee credentials, etc.
- Detect PII exposure to gain information on leaked PII such as login credentials, and financial details.
- Gain instant alerts whenever leaked credentials and critical information are found on the deep web or dark web.



Product highlights

Gain in-depth threat hunting through reengineered detection engine, which incorporates advanced detection logic, MITRE ATT&CK mapping, threat intelligence insights, and contextual analytics.

Detect anomalous and high-risk activity across users, devices, and applications using behavioral signals.

Monitor access to sensitive data and detect potential misuse or exfiltration through continuous activity analysis.

Identify shadow IT, policy violations, and risky behavior across cloud applications and services.

Standardize incident handling with native SOAR and prebuilt response workflows.

Simplify compliance audits with built-in reports and continuous log-based compliance monitoring.