LogZilla vs ManageEngine Log360

Product Comparison | December 2025

Executive Summary

LogZilla is not limited to log management or SIEM pre-processing. It provides full SIEM capabilities including threat detection, compliance reporting, SOAR automation, and AI-powered analysis that Log360 cannot match.

Common Misconceptions

LogZilla Platform Capabilities

Full SIEM Platform: LogZilla is a complete operational intelligence platform with full SIEM, SOAR automation, and AI-powered analysis. It can replace a SIEM entirely or work alongside one.

Deployment Options

Flexible Deployment: LogZilla offers Cloud SaaS (logzilla.cloud), Self-Hosted Linux, Kubernetes, VMware, and Air-Gapped deployments.

Compliance Capabilities

Full Compliance: LogZilla provides PCI DSS, HIPAA, GDPR, and SOX compliance with raw message preservation, audit trails, and automated reporting.

AI Domain Coverage

Domain	LogZilla AI	Log360
SecOps	IOCs, MITRE ATT&CK, attack chains	No
NetOps	Topology, cascading failures, CLI	No
InfraOps	Risk, outage prediction, capacity	No
AppOps	Error trends, dependencies	No
CloudOps	AWS/Azure/GCP/K8s correlation	No
Compliance	Evidence, framework mapping	No

Log360 Limitations

- Complex setup requiring significant configuration
- No natural language AI analysis
- UEBA, compliance packs cost extra
- Not designed for extreme log volumes
- No Kubernetes support for horizontal scaling

Threat Detection Comparison

Capability	LogZilla	Log360
Real-time correlation	Yes (stateless + stateful)	Yes
Brute force detection	Yes (threshold-based)	Yes
Lateral movement detection	Yes	Limited
APT detection	Yes (multi-stage)	Limited
Impossible travel	Yes	Requires UEBA add-on
AI-powered analysis	Yes (natural language)	No
Custom correlation rules	Unlimited	Limited

Real-World AI Example: Network Operations

Prompt: "Generate an incident report for the last 2 hours. Compare against yesterday's baseline. Include anomaly detection, priority matrix, and vendor-specific remediation commands."

AI-Generated Priority Matrix

Priority	Issue	Root Cause	Confidence
P1	PKI Certificate Failures	CA server unreachable	95%
P1	AD Connector Failures	DNS resolution failure	90%
P2	Wireless Auth Failures	EAP session timeouts	80%

Anomaly Detection (vs 24hr Baseline)

Metric	Current	Baseline	Delta
Total Events	5.06M	3.90M	+29.6%
Critical Events	273	231	+18.2%

Top Error-Generating Devices

Device	Error Count	Primary Issue
dhcp-primary	76,772	DHCP service errors
WLC-CORP-01	92,734	Auth failures
ise-node-03	1,617	AD connector errors

AI-Generated Remediation Commands

```
# Cisco IOS - Check certificate status
show crypto pki trustpoints
crypto pki authenticate sdn-network-infra-iwan
```

SOAR Capabilities Comparison

Feature	LogZilla	Log360
Built-in SOAR	Yes (years of production use)	Yes
Custom Script Execution	Full event context via environment variables	Limited
Webhook Integration	Any API endpoint	Limited integrations
Interactive Automation	Slack buttons, human-in-the-loop	No
Auto-Remediation	SSH to devices, restart services, block IPs	Playbook-based

Key Value Propositions

Eliminate Operations Overload

Collapse duplicates, filter noise. Existing teams support higher-tempo operations.

See Context, Not Noise

Enrich with topology and metadata. See impact and root cause instantly.

Turbocharge Existing SIEMs

Pre-process to cut volume 60-80%. Reduce license costs.

Key Differentiators

Full SIEM Capabilities

Real-time threat detection, event correlation, compliance reporting, SOAR automation, and AI-powered analysis.

Advanced AI Analysis

Natural language incident reports, root cause analysis, and vendor-specific remediation commands.

Built-In Compliance

PCI DSS, HIPAA, GDPR, SOX support with raw message preservation, audit storage, and automated reporting.

Enterprise Scale

10TB/day on single server; 230TB/day on Kubernetes. Patented deduplication (US #8,775,584).

Contact: sales@logzilla.net | www.logzilla.net