LogZilla vs Logpoint: Product Comparison

Product Comparison | December 2025

Executive Summary

Logpoint is a European SIEM with strong compliance focus, but its **limited AI capabilities, scaling challenges, and restricted integrations** create gaps. LogZilla delivers superior performance with AI-powered analysis and full SOAR automation.

Performance: LogZilla Wins

Metric	LogZilla	Logpoint
Single Server	10 TB/day	Stability issues at scale
Kubernetes	230 TB/day	No
Deduplication	Patented	No
Deployment	Minutes (Docker)	Complex setup

Logpoint Limitations

- Stability issues in large environments
- Limited third-party integrations
- No Kubernetes support
- Complex deployment process

AI Capabilities: LogZilla Wins

Capability	LogZilla	Logpoint
Natural Language	Yes	No
AI Reports	Executive summaries	Manual queries
Remediation	Vendor-specific CLI	Playbook-based
Air-Gapped AI	Ollama	No

Deployment Options

Option	LogZilla	Logpoint
Cloud SaaS	Yes	Yes
Kubernetes	Yes	No
Air-Gapped	Yes	No

AI Domain Coverage

Domain	LogZilla AI	Logpoint
SecOps	Threat intel, IOC extraction, MITRE ATT&CK mapping, attack correlation	Manual query
NetOps	Topology impact, cascading failure analysis, vendor-specific CLI commands	Manual query
InfraOps	Risk assessment, outage prediction, capacity analysis	Manual query
AppOps	Error rate trends, dependency mapping, performance analysis	Manual query
CloudOps	Cross-cloud correlation (AWS/Azure/GCP/K8s), resource drift	Manual query
Compliance	Evidence collection, policy violations, framework mapping	Manual query

SOAR Capabilities: LogZilla Wins

Feature	LogZilla	Logpoint
Built-in SOAR	Yes	Separate module
Custom Scripts	Full event context	Limited
Interactive	Human-in-the-loop	No
Auto-Remediation	SSH, restart, block	Playbook-based

LogZilla SOAR Advantages

- Execute custom scripts with full event context
- Interactive automation (Slack buttons, approvals)
- Auto-remediation (SSH, restart services, block IPs)
- Universal integration (ANY API or webhook)

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, cross-device correlation, 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%
P3	STP Loop Guard Flapping	Physical layer issue	70%

Anomaly Detection (vs 24hr Baseline)

Metric	Current	Baseline	Delta
Total Events	5.06M	3.90M	+29.6%
Critical Events	273	231	+18.2%
Avg Events/5min	222K	163K	+36.3%

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

# Cisco – Diagnose interface flapping
show interface GigabitEthernet1/0/24
show spanning-tree interface Gi1/0/24 detail
```

Event Correlation

Type	Capability
Stateless	Real-time matching, instant actions, webhooks
Stateful	Multi-event patterns, thresholds, attack chains
Advanced	Brute force, APT, impossible travel, lateral movement

Deployment Flexibility

Option	LogZilla	Logpoint
Cloud SaaS	Yes	Yes
Kubernetes	Yes	No
Air-Gapped	Yes	No

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

Advanced AI Capabilities

Executive summaries, priority matrices, vendor-specific CLI commands, and baseline anomaly detection.

Enterprise Scale

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

Integrated SOAR

Custom scripts, interactive automation, and auto-remediation. Integrates with ServiceNow, PagerDuty, Slack, Teams, and webhooks.

Cost Efficiency

60-80% SIEM cost reduction through transparent events/day pricing with unlimited users.