LogZilla vs Graylog: Product Comparison

Product Comparison | December 2025

Executive Summary

Graylog is popular for its open-source flexibility, but **limited enterprise features, no SOAR, and no AI capabilities** create gaps. LogZilla delivers superior performance with built-in SIEM, SOAR, and AI at **10x better performance**.

Enterprise Features: LogZilla Wins

Feature	LogZilla	Graylog
SIEM	Built-in	Security (paid add-on)
SOAR	Built-in	Not available
AI Analysis	Natural language	Not available
Compliance	Framework mapping	Basic reports

Graylog Pain Points

- Open source lacks enterprise security
- Graylog Security requires extra licensing
- No SOAR at any tier
- No AI-powered analysis

Performance: LogZilla Wins at Scale

Metric	LogZilla	Graylog
Single Server	10TB/day	~1TB/day typical
Kubernetes	230TB/day	Limited scaling
Deduplication	Yes (patented)	No
Storage	80-95% reduction	Full storage

Graylog Pain Points

- Elasticsearch backend limits scaling
- No deduplication = high storage
- Performance degrades at volume
- Cluster management complexity

AI Capabilities: LogZilla Wins (Graylog Has None)

Capability	LogZilla	Graylog
Natural Language Queries	Yes plain English	Not available
AI-Generated Reports	Executive summaries, compliance	Not available
Root Cause Analysis	Automatic with confidence scores	Manual
Remediation Commands	Vendor-specific CLI commands	Not available
Framework Mapping	CIS, NIST, ISO, PCI-DSS automatic	Not available

Real-World AI Example: Compliance Operations

Prompt: "Generate a compliance audit report for the last 24 hours. Include control effectiveness, policy violations, and evidence collection."

LogZilla AI Response (analyzing 13.6M events for compliance in seconds)

Control Effectiveness Summary

Framework	Tested	Passing	Coverage
PCI-DSS 4.0	64	58	91%
SOC 2 Type II	42	40	95%
HIPAA	28	26	93%

Policy Violations Detected

Policy	Violations	Severity
Password expiration	23 accounts	High
Privileged access	5 overdue	Medium
Patch compliance	12 systems	High

AI-Generated Evidence (PCI-DSS Req 10)

```
## 10.1 – Audit Trail Implementation
– Systems with logging: 847/847 (100%)
– Log forwarding to SIEM: 847/847 (100%)
– Average log latency: 2.3 seconds

## 10.2 – Automated Audit Trails
– User access events: 12,847,293
– Admin actions logged: 234,567
– Security events: 1,234,567
```

Access Control Evidence

User	Role	Status
admin_jsmith	DBA	Compliant
svc_backup	Service	Review
admin_mjones	NetAdmin	Compliant

In Graylog: *No compliance mapping, no evidence collection, manual report building.*

Migration Benefits

Benefit	Impact
Feature Upgrade	SIEM + SOAR + AI in one
Performance	10x over Elasticsearch
Storage	80-95% reduction
Operations	No ES cluster to manage

Easy Migration Path

- **Familiar Ingestion**: Same syslog-based approach
- **Similar Concepts**: Dashboards, alerts, streams
- **Better Performance**: Immediate improvement
- **Enterprise Features**: SOAR and AI included

Key Value Propositions

All Features Included

SIEM, SOAR, AI in base product. No add-on licensing.

10x Performance

No Elasticsearch dependency. Patented deduplication.

Compliance Ready

Framework mapping, evidence collection, audit reports.

Key Differentiators

Complete Platform

LogZilla includes SIEM, SOAR, and AI capabilities in the base product without add-on licensing.

Simplified Architecture

No Elasticsearch dependency. LogZilla's architecture eliminates cluster management complexity.

Built-in AI Analysis

Natural language queries generate compliance evidence and remediation commands automatically.

Automated Compliance

Framework mapping and evidence collection reduce audit preparation from days to minutes.

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