LogZilla vs Elastic (ELK Stack): Product Comparison

Product Comparison | December 2025

Executive Summary

Elastic (ELK Stack) is popular for its open-source roots, but **operational complexity, scaling challenges, and lack of built-in AI** create significant gaps. LogZilla delivers superior performance, built-in SIEM/SOAR, and AI-powered analysis with **50-70% lower TCO**.

Operational Simplicity: LogZilla Wins

Factor	LogZilla	Elastic
Deployment	Single Docker command	4+ components required
Cluster Mgmt	Automatic	Manual shard mgmt
Scaling	Kubernetes-native	Complex coordination
Maintenance	Minimal	Index lifecycle, heap tuning

Elastic Pain Points

- Requires dedicated Elastic expertise (expensive)
- Shard management is complex and error-prone
- JVM heap tuning requires constant attention
- Index lifecycle management adds burden

Performance: LogZilla Wins at Scale

Metric	LogZilla	Elastic
Single Server	10TB/day	~2TB/day (tuned)
Kubernetes	230TB/day	Massive cluster required
Storage	80-95% reduction	No deduplication
Query Speed	Sub-second	Depends on shards/heap

Elastic Pain Points

- Performance degrades without careful tuning
- Hot/warm/cold architecture adds complexity
- Large indices slow down searches
- Memory pressure causes instability

AI Capabilities: LogZilla Wins (Elastic Has No Equivalent)

Capability	LogZilla	Elastic
Natural Language Queries	Yes plain English	No requires KQL/Lucene
AI-Generated Reports	Executive summaries, compliance mapping	Not available
Root Cause Analysis	Automatic with confidence scores	Manual correlation
Remediation Commands	Vendor-specific CLI commands	Not available
Framework Mapping	CIS, NIST, ISO, PCI-DSS automatic	Manual tagging

Real-World AI Example: Application Operations

Prompt: "Generate an application health report for the last 24 hours. Correlate errors across microservices to identify root causes and dependency failures."

LogZilla AI Response (correlating 2.8M application events in seconds)

Error Summary by Service

Service	Errors	Rate	Top Error
payment-api	1,247	2.3%	DB timeout
user-auth	892	1.8%	Token expired
inventory-svc	456	0.9%	Cache miss

Root Cause Correlation

Symptom	Root Cause	Confidence
Checkout timeouts	DB pool exhausted	92%
Auth failures	Redis eviction	85%
Slow search	ES index fragmentation	78%

AI-Generated Remediation

```
# Database connection pool
SHOW STATUS LIKE 'Threads_connected';
SET GLOBAL max_connections = 500;

# Redis cache diagnostics
redis-cli INFO memory
redis-cli CONFIG SET maxmemory-policy allkeys-lru

# Elasticsearch index health
GET _cluster/health
POST /search-index/_forcemerge
```

Performance Analysis

Endpoint	Avg	P95
/api/checkout	2.4s	8.7s
/api/search	180ms	450ms
/api/auth	340ms	890ms

In Elastic: *Requires APM (separate product), custom dashboards, no root cause correlation or remediation.*

SIEM/SOAR Comparison

Feature	LogZilla	Elastic Security
SIEM Included	Yes (built-in)	Add-on license
SOAR Included	Yes (built-in)	No
Detection Rules	Pre-built + custom	Requires config
Automated Response	Full scripting	Limited

LogZilla + Elastic (Complement)

For customers heavily invested in Elastic:

- **Pre-Processor**: Reduce Elastic ingest 60-80%
- **AI Layer**: Add natural language analysis
- **Real-time Alerting**: Handle correlation in LogZilla
- **Gradual Migration**: Move workloads over time

Key Value Propositions

50-70% Lower TCO

No Elastic expertise needed. No Platinum license. 80-95% storage reduction.

AI That Elastic Can't Match

Natural language queries, compliance mapping, automated remediation commands.

Zero Operational Burden

No shard management. No heap tuning. No index lifecycle complexity.

Key Differentiators

Operational Simplicity

No shard management, heap tuning, or index lifecycle complexity. LogZilla deploys in minutes and scales automatically.

Enterprise Scale

Handle 230TB/day with automatic scaling. No cluster management overhead or performance degradation at scale.

Built-in AI Analysis

Natural language queries generate compliance reports with remediation commands—capabilities Elastic doesn't offer natively.

Lower Total Cost

50-70% TCO reduction when factoring in expertise requirements, Platinum licensing, and storage costs.

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