LogZilla vs Splunk: Product Comparison

Product Comparison | December 2025

Executive Summary

Splunk is the market leader in log management and Security Information and Event Management (SIEM), but its licensing costs, complexity, and resource requirements create significant pain points. LogZilla offers comparable capabilities at **60-80% lower cost**, plus AI-powered analysis that Splunk cannot match.

Cost Comparison: LogZilla Wins

Factor	LogZilla	Splunk
Licensing Model	Events/day (predictable)	GB/day (unpredictable)
Typical Savings	60-80%	Baseline
Hidden Costs	None	Apps, training, services
User Licensing	Unlimited	Per-user fees

Splunk Pain Points

- Customers exceed GB/day limits, triggering overage charges
- "Splunk tax": apps, add-ons, professional services
- Complex pricing tiers (Workload, Ingest, Entity)
- Sticker shock at renewal

Performance: LogZilla Wins at Scale

Metric	LogZilla	Splunk
Single Server	10TB/day	~500GB/day typical
Kubernetes	230TB/day	Expensive clustering
Deployment	Minutes (Docker)	Days to weeks
Efficiency	10x more efficient	Heavy resources

Splunk Pain Points

- Significant hardware investment required
- Complex distributed deployments
- Search performance degrades with volume
- Indexer clustering is expensive

AI Capabilities: LogZilla Wins (Splunk Has No Equivalent)

Capability	LogZilla	Splunk
Natural Language Queries	Yes plain English	No requires SPL
AI-Generated Reports	Executive summaries, priority matrices	Manual dashboard building
Root Cause Analysis	Automatic with confidence scores	Manual correlation
Remediation Commands	Vendor-specific CLI commands	Not available
Baseline Comparison	Automatic anomaly detection	Requires ML Toolkit setup

Why Splunk Customers Switch

Common Splunk Frustrations

- **Budget overruns**: GB/day pricing leads to surprise bills
- **SPL complexity**: Steep learning curve, requires specialists
- **Renewal shock**: 20-40% annual price increases
- **Resource demands**: Heavy infrastructure requirements
- **Slow searches**: Performance degrades at scale

LogZilla Solves These Problems

- **Predictable pricing**: Events/day, no overages
- **No query language**: Ask in plain English
- **60-80% savings**: Immediate cost reduction
- **10x efficiency**: Less hardware required
- **Sub-second queries**: Even at 10TB/day

Real-World AI Example: Security Operations

Prompt: "Generate a security incident report for the last hour. Include threat detection, attack correlation, framework mapping, and remediation priorities."

LogZilla AI Response (13.6M events analyzed in seconds)

Threat Detection Summary

Source IP	Attack Type	Severity
184.147.253.223	Brute Force (root)	CRITICAL
55.53.163.17	Brute Force (multi)	CRITICAL
200.176.232.83	Account Enumeration	HIGH

Framework Compliance Mapping

Control	Status	Gap
CIS 4.3	FAIL	Root access not blocked
NIST AC-7	FAIL	No account lockout
ISO A.9.4.2	PARTIAL	Weak auth tolerance

AI-Generated Remediation

```
# Block attacking IPs immediately
iptables -A INPUT -s 184.147.253.223 -j DROP
iptables -A INPUT -s 55.53.163.17 -j DROP

# Enable fail2ban for SSH
fail2ban-client set sshd banip 184.147.253.223

# Cisco ASA - Block at perimeter
access-list OUTSIDE deny ip host 184.147.253.223 any
```

Compliance Scorecard

Framework	Score
CIS Controls v8	58%
NIST 800-53	67%
ISO 27001	62%

***In Splunk:** Requires separate SOAR ($50K+), manual SPL queries, and no framework mapping.*

SOAR Comparison

Feature	LogZilla	Splunk SOAR
Included	Yes (built-in)	Separate product
Pricing	Included	$50K+ starting
Custom Scripts	Full event context	Playbook-based
Learning Curve	Hours	Weeks

LogZilla as Splunk Pre-Processor

For customers not ready to replace Splunk:

- **Reduce Splunk ingest 60-80%**: deduplicate before forwarding
- **Real-time analysis**: handle alerting in LogZilla
- **Add AI capabilities**: Splunk doesn't have
- **Migrate gradually**: if desired

Key Value Propositions

60-80% Cost Savings

Predictable events/day pricing. No surprise overages. Unlimited users included.

AI That Splunk Can't Match

Natural language queries, auto-generated reports, vendor-specific remediation commands.

10x Performance

Single server handles what requires Splunk cluster. Patented deduplication (US #8,775,584).

Key Differentiators

Significant Cost Savings

Organizations typically achieve 60-80% cost reduction compared to Splunk through predictable events/day pricing and patented deduplication.

AI-Powered Analysis

Natural language queries and AI-generated remediation commands eliminate the need for SPL expertise and manual correlation.

Simplified Operations

Deploy in minutes with Docker. Single-server performance that rivals Splunk clusters, reducing infrastructure complexity.

Flexible Integration

Use as a complete Splunk replacement or as a pre-processor to reduce Splunk ingest costs while adding AI capabilities.

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