LogZilla vs LogRhythm: Product Comparison

Product Comparison | December 2025

Executive Summary

LogRhythm is a traditional SIEM with on-premises heritage, but its **aging architecture, complex deployment, and limited AI** create gaps. LogZilla delivers modern architecture with **50-70% lower TCO** and AI-powered analysis.

Modern Architecture: LogZilla Wins

Factor	LogZilla	LogRhythm
Architecture	Cloud-native, containerized	Traditional, appliance
Deployment	Minutes (Docker)	Days to weeks
Scaling	Kubernetes (230TB/day)	Appliance additions
Maintenance	Minimal	Significant overhead

LogRhythm Pain Points

- Legacy appliance-based architecture
- Scaling requires more hardware
- Complex deployment and config
- High maintenance overhead

Performance: LogZilla Wins

Metric	LogZilla	LogRhythm
Single Server	10TB/day	Appliance-dependent
Deduplication	Yes (patented)	No
Storage	80-95% reduction	Standard
Query Speed	Sub-second	Varies with volume

LogRhythm Pain Points

- Performance limited by appliances
- No deduplication = high storage
- Query performance degrades
- Hardware refresh cycles expensive

AI Capabilities: LogZilla Wins

Capability	LogZilla	LogRhythm
Natural Language Queries	Yes plain English	No query builder
AI-Generated Reports	Executive summaries, compliance	Limited AI features
Remediation Commands	Vendor-specific CLI	Playbook-based (manual)
MITRE ATT&CK	Automatic mapping	Manual tagging

TCO Comparison

Factor	LogZilla	LogRhythm
Licensing	Events/day	Appliance + MPS
Hardware	Commodity	Dedicated appliances
SOAR	Included	SmartResponse (limited)
Services	Minimal	Often required

LogRhythm Customer Pain Points

- "Appliance model feels outdated"
- "Scaling requires more hardware"
- "We need dedicated LogRhythm admins"
- "Upgrades are painful"

Real-World AI Example: Infrastructure Operations

Prompt: "Generate a network operations report. Include PKI certificate status, auth failures, and baseline comparison."

LogZilla AI Response (analyzing 5.06M events in 2.8 seconds)

Incident Priority Matrix

Priority	Issue	Confidence	Events
P1	PKI Cert Renewal Failure	95%	273
P1	AD Connector Failure	90%	1,617
P2	Wireless Auth Failures	80%	92,734

Anomaly Detection - Baseline

Metric	Current	Baseline	Delta
Total Events	5.06M	3.90M	+29.6%
Critical Events	273	231	+18.2%
Avg/5min	221K	162K	+36.3%

AI-Generated Remediation

```
# Verify CA Server Status (Cisco)
show crypto pki trustpoints
show crypto pki certificates sdn-network-infra-iwan

# Test connectivity to CA
nslookup
telnet  443

# ISE AD Connector Recovery
ise-psn# application configure ise
# Select option 29: Rejoin Active Directory
```

Replacement Opportunity

- **Modernization**: Appliances to containers
- **AI Upgrade**: Natural language + baseline
- **Cost**: 50-70% TCO savings

In LogRhythm: *No baseline comparison, no network device commands.*

Key Value Propositions

Modern Architecture

Containerized, Kubernetes-native. No appliances.

50-70% Lower TCO

No appliances, less hardware, minimal services.

AI-Powered Analysis

Natural language, MITRE mapping, remediation commands.

Key Differentiators

Modern Architecture

Containerized, Kubernetes-native deployment eliminates appliance dependencies and simplifies scaling.

AI-Powered Analysis

Natural language queries with automatic MITRE ATT&CK mapping and vendor-specific remediation commands.

Lower Total Cost

50-70% TCO reduction through elimination of appliances, reduced hardware, and minimal professional services.

Simplified Operations

Deploy in minutes with Docker. Minimal ongoing maintenance compared to traditional SIEM platforms.

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