# LogZilla vs Sumo Logic: Product Comparison

**Product Comparison | December 2025**

## Executive Summary

Sumo Logic is a cloud-native log management platform, but its **credit-based pricing, cloud-only deployment, and limited automation** create gaps. LogZilla delivers superior performance with built-in SOAR and AI at **predictable pricing**.

## Cost: LogZilla Wins Predictability

| Factor | LogZilla | Sumo Logic |
|---|---|---|
| Pricing Model | Events/day (predictable) | Credits (consumption) |
| Ingest Pricing | Included | Credits per GB |
| Storage | 80-95% reduction | Full storage costs |
| Users | Unlimited | Included in credits |

### Sumo Logic Pain Points

- Credit consumption difficult to predict
- High-volume burns credits quickly
- No deduplication = higher costs
- Budgeting is challenging

## Deployment: LogZilla Wins Flexibility

| Option | LogZilla | Sumo Logic |
|---|---|---|
| Cloud SaaS | Yes | Yes (only option) |
| Self-Hosted | Yes | No |
| Air-Gapped | Yes | No |
| Hybrid | Yes | No |

### Sumo Logic Pain Points

- Cloud-only: no air-gapped option
- Compliance needs on-premises
- No data residency control
- Query performance varies

## AI Capabilities: LogZilla Wins

| Capability | LogZilla | Sumo Logic |
|---|---|---|
| Natural Language Queries | Yes plain English | No requires query syntax |
| AI-Generated Reports | Executive summaries, compliance | Limited ML features |
| Root Cause Analysis | Automatic with confidence scores | Root Cause Explorer (basic) |
| Remediation Commands | Vendor-specific CLI commands | Not available |
| Framework Mapping | CIS, NIST, ISO, PCI-DSS automatic | Manual configuration |

## Performance Comparison

| Metric | LogZilla | Sumo Logic |
|---|---|---|
| Single Server | 10 TB/day | Cloud-dependent |
| Kubernetes | 230 TB/day | No |
| Deduplication | Patented | No |
| Storage Savings | 80-95% | Standard |

### Why Sumo Logic Customers Switch

- **Credit burn**: Unpredictable consumption
- **Cloud-only**: No on-premises option
- **Query syntax**: Learning curve required
- **No deduplication**: Higher storage costs

## Real-World AI Example: Network Operations

*Prompt: "Generate an incident report for the last 2 hours. Compare against yesterday's baseline. Include anomaly detection and remediation commands."*

**LogZilla AI Response** (analyzing 5M+ network events in seconds)

### Priority Matrix

| Priority | Issue | Root Cause | Confidence |
|---|---|---|---|
| P1 | PKI Cert Failures | CA unreachable | 95% |
| P1 | AD Connector Failures | DNS failure | 90% |
| P2 | Wireless Auth | EAP timeouts | 80% |

### Anomaly Detection (vs 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% |

### AI-Generated Remediation

```
# 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

# Juniper: BGP troubleshooting
show bgp neighbor
show bgp summary
```

### Top Error Devices

| Device | Errors | Issue |
|---|---|---|
| dhcp-primary | 76,772 | DHCP errors |
| WLC-CORP-01 | 92,734 | Auth failures |
| ise-node-03 | 1,617 | AD connector |

***In Sumo Logic:** Manual queries, no baseline comparison, no remediation commands.*

## SOAR Comparison

| Feature | LogZilla | Sumo Logic |
|---|---|---|
| SOAR Included | Yes (built-in) | Cloud SOAR (extra) |
| Custom Scripts | Full event context | Playbook-based |
| Integration | Any API/webhook | Pre-built connectors |
| Learning Curve | Hours | Days to weeks |

### LogZilla + Sumo Logic (Complement)

*For customers invested in Sumo Logic:*

- **Pre-Processor**: Reduce credit consumption 60-80%
- **AI Layer**: Natural language analysis
- **SOAR**: Built-in without Cloud SOAR cost
- **Air-Gapped**: Handle regulated environments

## Key Value Propositions

### Predictable Pricing

*Events/day model. No credit surprises. 80-95% storage reduction.*

### Deploy Anywhere

*Cloud, on-premises, air-gapped, hybrid. Sumo Logic is cloud-only.*

### AI + SOAR Built-In

*Natural language queries, automated response, compliance mapping.*

## Key Differentiators

### Predictable Pricing

*Transparent events/day pricing eliminates credit-based consumption surprises and budget overruns.*

### AI-Powered Remediation

*Natural language queries generate vendor-specific remediation commands and compliance evidence.*

### Flexible Deployment

*Deploy on-premises, air-gapped, or hybrid environments. No cloud dependency required.*

### Pre-Processor Option

*LogZilla deduplication can reduce Sumo Logic credit consumption by 60-80% when used as a pre-processor.*

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