LogZilla vs Devo: Product Comparison

Product Comparison | December 2025

Executive Summary

Devo is a cloud-native SIEM focused on high-volume data, but its **cloud-only deployment, LINQ complexity, and limited SOAR** create gaps. LogZilla delivers **deployment flexibility** and natural language AI.

Deployment: LogZilla Wins Flexibility

Option	LogZilla	Devo
Cloud SaaS	Yes	Yes (primary)
Self-Hosted	Yes	No
Air-Gapped	Yes	No
Kubernetes	230TB/day	No

Devo Pain Points

- Cloud-only limits deployment options
- No air-gapped capability
- Data residency concerns
- LINQ query language complexity

Cost: LogZilla Wins Predictability

Factor	LogZilla	Devo
Pricing	Events/day	GB/day ingestion
Deduplication	Yes (patented)	No
Storage	80-95% reduction	Standard compression
SOAR	Included	Devo SOAR (extra)

Devo Pain Points

- GB-based pricing scales with volume
- No deduplication = higher costs
- SOAR requires additional licensing
- Costs can be unpredictable

AI Capabilities: LogZilla Wins

Capability	LogZilla	Devo
Natural Language Queries	Yes plain English	No LINQ required
Analysis Scope	SecOps, NetOps, InfraOps, AppOps, CloudOps	Security-focused
Remediation Commands	Vendor-specific CLI	Not available
MITRE ATT&CK	Automatic mapping	Manual tagging

Real-World AI Example: DNS Attack Analysis

Prompt: "Analyze DNS security events. Include attack patterns, source IPs, and Infoblox remediation."

> **LogZilla AI Response** (analyzing 13.6M events in 4.1 seconds)

DNS Attack Detection

Finding	Confidence	Events
DNS Amplification	95%	20+
IP Spoofing via DNS	90%	13
DNS Tunneling (C2)	85%	347

Attack Source Analysis

Source IP	Attack Type	Action
203.0.113.83	Amplification	Rate Limited
45.142.xxx.xxx	DNS Tunneling	Blocked
185.220.xxx.xxx	Exfiltration	Blocked

AI-Generated Remediation

```
# Infoblox: Enable DNS RRL
set rrl enable
set rrl responses-per-second 5

# Infoblox: Block amplification sources
set blacklist add 203.0.113.0/24

# Cisco ASA: Block DNS amplification
access-list OUTSIDE_IN deny udp any host ns1 eq 53
```

LogZilla + Devo (Complement)

For customers invested in Devo:

- **On-Premises**: Air-gapped/regulated
- **Cost**: Reduce ingest with deduplication
- **AI**: Natural language queries

In Devo: *LINQ queries, no Infoblox commands.*

SOAR Comparison

Feature	LogZilla	Devo
SOAR Included	Yes (built-in)	Devo SOAR (separate)
Automation	Full scripting	Playbook-based
Pricing	Included	Additional cost
Integration	Any API/webhook	Pre-built connectors

Devo Customer Pain Points

- "Cloud-only doesn't meet compliance needs"
- "LINQ has a steep learning curve"
- "GB-based pricing gets expensive"
- "SOAR is an additional expense"

Key Value Propositions

Deploy Anywhere

Cloud, on-premises, air-gapped. Devo is cloud-only.

Natural Language AI

Plain English queries. No LINQ required.

SOAR + Deduplication

Built-in SOAR. 80-95% storage reduction.

Key Differentiators

Deployment Flexibility

LogZilla deploys on-premises, air-gapped, or hybrid environments. No cloud dependency required.

Natural Language Queries

Plain English queries eliminate the need to learn proprietary query languages like LINQ.

Cost Efficiency

Patented deduplication provides 80-95% storage reduction with predictable events/day pricing.

Integrated SOAR

SOAR capabilities included in the base platform rather than requiring separate licensing.

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