LogZilla vs IBM QRadar: Product Comparison

Product Comparison | December 2025

Executive Summary

IBM QRadar is an established enterprise SIEM, but its **complexity, high TCO, and lack of modern AI** create gaps. LogZilla delivers superior performance, simpler deployment, and AI-powered analysis with **50-70% lower TCO**.

Simplicity: LogZilla Wins

Factor	LogZilla	QRadar
Deployment	Minutes (Docker)	Weeks to months
Architecture	Single platform	Multiple components
Administration	Minimal	Dedicated admin
Learning Curve	Hours	Weeks of training

QRadar Pain Points

- Complex multi-component architecture
- Requires dedicated QRadar expertise
- Lengthy deployment and tuning
- Steep learning curve (AQL)

Cost: LogZilla Wins on TCO

Factor	LogZilla	QRadar
Licensing	Events/day	EPS-based (complex)
Hardware	10TB/day single server	Heavy requirements
Services	Minimal	Often required
Training	Included	Expensive IBM training

QRadar Pain Points

- EPS licensing complex and expensive
- Significant hardware investment
- Professional services often needed
- Ongoing training costs

AI Capabilities: LogZilla Wins

Capability	LogZilla	QRadar
Natural Language Queries	Yes plain English	No AQL required
AI-Generated Reports	Executive summaries, compliance	Watson (deprecated)
Root Cause Analysis	Automatic with confidence scores	Manual investigation
Remediation Commands	Vendor-specific CLI commands	Not available
MITRE ATT&CK Mapping	Automatic	Manual tagging

Real-World AI Example: Security Operations

Prompt: "Generate a security incident report for the last 24 hours. Include threat intelligence, MITRE ATT&CK mapping, and remediation commands."

LogZilla AI Response (analyzing 13.6M security events in seconds)

Threat Intelligence: Top Attackers

Source IP	Country	Threat Type
45.142.xxx.xxx	Russia	Brute Force
185.220.xxx.xxx	Germany	Port Scan
23.94.xxx.xxx	US	DNS Amplification

MITRE ATT&CK Mapping

Technique	Tactic	Evidence
T1110.001	Credential Access	12,453 SSH failures
T1498.002	Impact	DNS amplification
T1046	Discovery	Port scanning

AI-Generated Remediation

```
# Cisco ASA: Block attacker
access-list OUTSIDE_IN deny ip host 45.142.xxx.xxx any

# Palo Alto: Create EDL block
set address "Threat-Actor-1" ip-netmask 45.142.xxx.xxx/32
set security policy deny-threats source "Threat-Actor-1"

# Fortinet: Block and log
config firewall address
  edit "blocked-attacker"
  set subnet 45.142.xxx.xxx/32
end
```

Executive Summary

Finding	Severity	Count
DNS Amplification	Critical	847
SSH Brute Force	High	12,453
Firewall Denies	Medium	156,892

In QRadar: *Manual AQL queries, no MITRE mapping, no remediation commands.*

SOAR Comparison

Feature	LogZilla	QRadar SOAR
Included	Yes (built-in)	Separate product
Pricing	Included	Significant extra cost
Integration	Native	Requires configuration
Complexity	Simple scripting	Playbook development

Migration Benefits

- **Simplification**: Single platform vs multi-component
- **Cost Reduction**: 50-70% TCO savings typical
- **AI Upgrade**: Natural language vs AQL
- **SOAR Included**: No separate product needed

Key Value Propositions

50-70% Lower TCO

Simpler licensing, less hardware, no expensive services.

Minutes vs Months

Deploy in minutes. No weeks of tuning required.

Modern AI Built-In

Natural language, MITRE ATT&CK mapping, remediation commands.

Key Differentiators

Rapid Deployment

LogZilla deploys in minutes via Docker, compared to weeks or months for traditional QRadar implementations.

Lower Total Cost

50-70% TCO reduction through simpler licensing, reduced hardware requirements, and minimal professional services.

Modern AI Capabilities

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

Integrated SOAR

SOAR capabilities included in the base platform rather than requiring a separate product purchase.

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