LogZilla vs Microsoft Sentinel: Product Comparison

Product Comparison | December 2025

Executive Summary

Microsoft Sentinel is Azure-native SIEM, but its **Azure dependency, unpredictable costs, and limited multi-vendor support** create gaps. LogZilla delivers superior flexibility with **predictable pricing** and vendor-neutral AI.

Deployment: LogZilla Wins Flexibility

Option	LogZilla	Sentinel
Cloud Provider	AWS, Azure, GCP, or on-prem	Azure only
Self-Hosted	Yes	No
Air-Gapped	Yes	No
Multi-Cloud	Native	Azure-centric

Sentinel Pain Points

- Requires Azure subscription
- No self-hosted or air-gapped option
- Azure-centric limits flexibility
- Non-Microsoft logs are second-class

Cost: LogZilla Wins Predictability

Factor	LogZilla	Sentinel
Pricing	Events/day	GB ingested + retention
Predictability	High	Low
Retention	Included	90 days free, then paid
Commitment	Flexible	Reservations for discounts

Sentinel Pain Points

- Costs scale unpredictably
- Long-term retention expensive
- Capacity reservations required
- Azure consumption adds up

AI Capabilities: LogZilla Wins Multi-Vendor

Capability	LogZilla	Sentinel
Natural Language Queries	Yes plain English	Copilot for Security (extra cost)
Multi-Vendor Remediation	Cisco, Juniper, VMware, Linux	Azure/Microsoft focused
Root Cause Analysis	Automatic with confidence scores	Manual investigation
Query Syntax	Natural language	KQL required

Performance Comparison

Metric	LogZilla	Sentinel
Single Server	10 TB/day	Cloud-dependent
Kubernetes	230 TB/day	No
Deduplication	Patented	No
Air-Gapped	Yes	No

LogZilla Advantages

- Multi-vendor remediation commands
- No Azure lock-in or dependency
- Predictable events/day pricing
- Air-gapped deployment option

Real-World AI Example: Infrastructure Operations

Prompt: "Generate an infrastructure health report for the last 24 hours. Include server health across all environments and remediation commands."

LogZilla AI Response (analyzing 1,400+ systems across clouds in seconds)

Server Health Summary

Category	Healthy	Warning	Critical
Physical Servers	142	8	2
Virtual Machines	1,247	34	5
Storage Arrays	12	1	0

Critical Issues Identified

Server	Issue	Impact
db-prod-03	Disk 95% full	High
esxi-host-07	Memory overcommit	Medium
backup-srv-01	Job failures	High

AI-Generated Remediation

```
# Linux: Disk space analysis
df -h /var/lib/mysql
du -sh /var/lib/mysql/* | sort -hr | head -20

# VMware ESXi: Host diagnostics
esxcli system health status get
esxcli hardware memory get

# Windows: Service recovery
Get-Service | Where {$_.Status -eq 'Stopped'}
Get-EventLog -LogName System -EntryType Error
```

Resource Trending

Resource	Current	7-Day Avg
CPU (cluster)	67%	54%
Memory	78%	72%
Storage (SAN)	71%	68%

In Sentinel: *Azure Monitor + KQL required. No VMware/Linux remediation commands.*

SOAR Comparison

Feature	LogZilla	Sentinel
SOAR Included	Yes (built-in)	Logic Apps (separate)
Automation	Full scripting	Playbooks via Logic Apps
Pricing	Included	Logic Apps consumption
Complexity	Simple	Azure ecosystem knowledge

LogZilla + Sentinel (Complement)

For Microsoft-invested customers:

- **Multi-Cloud Logs**: AWS, GCP, on-premises
- **Cost Control**: Reduce Sentinel ingestion
- **AI Analysis**: Vendor-neutral queries
- **Air-Gapped**: Regulated environments

Key Value Propositions

No Vendor Lock-In

Deploy anywhere. Any cloud, on-premises, air-gapped.

Predictable Pricing

Events/day model. No consumption surprises.

Vendor-Neutral AI

Equal support for Cisco, VMware, Linux, Microsoft.

Key Differentiators

Deployment Flexibility

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

Predictable Pricing

Transparent events/day pricing model eliminates consumption-based cost surprises common with cloud SIEM.

Vendor-Neutral Support

Equal AI-powered analysis and remediation for Cisco, VMware, Linux, and Microsoft environments.

Complementary Option

LogZilla can handle non-Azure workloads while Sentinel focuses on Azure-native resources.

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