LogZilla vs Securonix: Product Comparison

Product Comparison | December 2025

Executive Summary

Securonix is a cloud-native SIEM with UEBA, but its **cloud-only deployment, complex pricing, and security-only focus** create gaps. LogZilla delivers **deployment flexibility** and broader AI analysis.

Deployment: LogZilla Wins Flexibility

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

Securonix Pain Points

- Cloud-native limits deployment options
- No air-gapped capability
- Data residency concerns
- Cloud availability dependency

Cost: LogZilla Wins Predictability

Factor	LogZilla	Securonix
Pricing	Events/day	EPS + users + storage
SOAR	Included	Add-on
UEBA/AI	Included	Core feature
Predictability	High	Complex tiers

Securonix Pain Points

- Complex multi-factor pricing
- SOAR requires additional licensing
- Costs scale unpredictably
- Premium features at premium prices

AI Capabilities: LogZilla Wins on Breadth

Capability	LogZilla	Securonix
Natural Language Queries	Yes plain English	No query syntax
Analysis Scope	SecOps, NetOps, InfraOps, AppOps, CloudOps	Security/UEBA focused
Remediation Commands	Vendor-specific CLI	Limited
MITRE ATT&CK	Automatic mapping	Supported

Performance Comparison

Metric	LogZilla	Securonix
Single Server	10 TB/day	Cloud-dependent
Kubernetes	230 TB/day	No
Deduplication	Patented	No
Storage Reduction	80-95%	Standard

LogZilla Advantages

- On-premises option for data sovereignty
- Air-gapped deployment with full AI
- Patented deduplication reduces storage
- Predictable events/day pricing

Real-World AI Example: Wireless Auth Analysis

Prompt: "Analyze wireless authentication failures. Include failure categories, affected users, and remediation."

LogZilla AI Response (analyzing 5.06M events in 3.1 seconds)

Authentication Failure Summary

Category	Count	Risk
Invalid Password	24,408	Critical
EAP Abandoned	5,440	High
Client Timeout	12,934	High

Root Cause Analysis

Issue	Confidence	Evidence
Credential Stuffing	85%	24K failures from 12 IPs
Supplicant Misconfig	70%	PEAP failures by device
RADIUS Latency	65%	Timeout correlation

AI-Generated Remediation

```
# Cisco WLC: Block attacking MACs
config exclusionlist add
config exclusionlist description  "Stuffing"

# Cisco ISE: Failed auth throttling
ise(config)# radius-server deadtime 5

# Investigate specific user
show client detail
debug client
```

Affected Users with Risk

User	Failures	Risk	Status
jsmith	847	92	INVESTIGATE
svc_wireless	234	78	REVIEW

In Securonix: *No wireless analysis, no WLC/ISE commands.*

Log Management + Complement Strategy

Feature	LogZilla	Securonix
Performance	10TB/day single	Cloud-dependent
Deduplication	Yes	No
Storage	80-95% reduction	Standard

LogZilla + Securonix

For customers invested in Securonix:

- **On-Premises**: Air-gapped/regulated
- **Network/Infra**: Visibility Securonix lacks
- **AI Breadth**: Natural language all domains
- **Cost**: Reduce Securonix data volume

Key Value Propositions

Deploy Anywhere

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

Broader AI Analysis

SecOps, NetOps, InfraOps, AppOps, CloudOps.

Predictable Pricing

Events/day. SOAR included. No complex tiers.

Key Differentiators

Deployment Flexibility

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

Broader AI Coverage

AI analysis spans security, network, infrastructure, applications, and cloud with vendor-specific remediation.

Transparent Pricing

Events/day pricing with SOAR included. No complex tiered licensing structures.

Natural Language Interface

Plain English queries generate analysis and remediation without specialized query syntax.

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