LogZilla vs Rapid7 InsightIDR: Product Comparison

Product Comparison | December 2025

Executive Summary

Rapid7 InsightIDR is a cloud-native SIEM with vulnerability management integration, but its **cloud-only deployment, security-only focus, and complex pricing** create gaps. LogZilla delivers **deployment flexibility** and broader AI analysis.

Deployment: LogZilla Wins Flexibility

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

InsightIDR Pain Points

- Cloud-only limits deployment options
- No air-gapped capability
- Data residency concerns
- Security-first, logs secondary

Log Management: LogZilla Wins

Feature	LogZilla	InsightIDR
Performance	10TB/day single	Cloud-dependent
Deduplication	Yes (patented)	No
Storage	80-95% reduction	Standard
Focus	Purpose-built logs	Security-first

InsightIDR Pain Points

- Log management is secondary
- No deduplication = higher costs
- Limited retention options
- Not designed for high-volume ops logs

AI Capabilities: LogZilla Wins on Breadth

Capability	LogZilla	Rapid7 InsightIDR
Natural Language Queries	Yes plain English	No query syntax
Analysis Scope	SecOps, NetOps, InfraOps, AppOps, CloudOps	Security-only
Remediation Commands	Vendor-specific CLI	Limited
MITRE ATT&CK	Automatic mapping	Supported

Real-World AI Example: Compliance Audit

Prompt: "Generate a compliance audit report. Correlate access logs, change records, and security events. Include framework mapping."

LogZilla AI Response (analyzing 13.6M events in 4.2 seconds)

Compliance Scorecard

Framework	Score	Status
CIS Controls v8	58%	Below Baseline
NIST 800-53	67%	Partial
ISO 27001:2022	62%	Partial
PCI-DSS 4.0	70%	Attention

Control Gap Analysis

Control	Status	Gap
CIS 4.3	FAILED	Root access not blocked
NIST AC-7	NON-COMPLIANT	No account lockout
ISO A.9.4.2	GAP	Multiple failures allowed

AI-Generated Remediation Priorities

Priority	Issue	Framework
P1	Block IPs, enable fail2ban	CIS 4.3, NIST AC-7
P1	Expand DHCP pools	CIS 11.2, ISO A.12.1.3
P2	Review privileged access	SOX-ITGC-04, PCI-DSS

LogZilla + Rapid7 (Complement)

For customers invested in Rapid7:

- **Log Management**: High-volume ops logs
- **On-Premises**: Air-gapped/regulated
- **Keep InsightVM**: Vulnerability scanning

In InsightIDR: *No natural language, limited multi-framework mapping.*

Cost Comparison

Factor	LogZilla	InsightIDR
Pricing	Events/day	Assets + data volume
SOAR	Included	InsightConnect (extra)
Predictability	High	Complex asset-based

InsightIDR Customer Pain Points

- "Asset-based pricing is hard to predict"
- "InsightConnect SOAR adds significant cost"
- "Great for security, limited for operations"
- "Cloud-only doesn't meet compliance needs"

Key Value Propositions

Deploy Anywhere

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

Broader AI Analysis

SecOps, NetOps, InfraOps, AppOps, CloudOps.

Purpose-Built Logs

80-95% deduplication. Security AND operations.

Key Differentiators

Deployment Flexibility

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

Broader AI Analysis

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

Purpose-Built Log Management

Designed for high-volume log management with 80-95% deduplication, handling both security and operational use cases.

Predictable Pricing

Events/day pricing model provides cost predictability compared to asset-based licensing.

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