LogZilla vs Cribl: Product Comparison

Product Comparison | December 2025

Executive Summary

Cribl is a data routing pipeline, **not a SIEM or log management solution**. Cribl routes data to destinations; LogZilla analyzes, stores, and acts on it. LogZilla's built-in deduplication **eliminates the need for Cribl**.

Critical Distinction: Cribl is a data pipeline. It still requires a destination (Splunk, Elastic, LogZilla) to store and analyze logs.

Capability Comparison

Capability	LogZilla	Cribl
Log Storage	Yes	No (routes only)
Log Analysis	AI-powered	No
SIEM	Built-in	No
SOAR	Built-in	No
Alerting	Yes	No

Why Cribl Exists

- Reduce costs of expensive SIEMs (Splunk)
- Route data to multiple destinations
- Filter/transform before storage

LogZilla's pricing and deduplication eliminate these needs.

Complete Solution: LogZilla Wins

Factor	LogZilla	Cribl + Destination
Products	1 platform	2+ products
Vendors	Single vendor	Multiple vendors
Complexity	Low	High
Cost	All-inclusive	Cribl + destination

Cribl Pain Points

- Still requires destination SIEM
- Two products to license and manage
- Adds architectural complexity
- Sampling loses data fidelity permanently

LogZilla provides complete functionality without a routing layer.

Data Reduction: LogZilla Eliminates the Need

Approach	LogZilla	Cribl + Destination
Deduplication	Built-in (patented)	Sampling (data loss)
Storage Reduction	80-95%	Varies by config
Data Loss Risk	None (full fidelity)	High (sampling discards data)
Compliance	Full retention	May filter required data

AI Capabilities: LogZilla Wins (Cribl Has None)

Capability	LogZilla	Cribl
Natural Language	Yes	N/A
AI Reports	Yes	N/A
Root Cause	Yes	N/A
Remediation	Yes	N/A

Cribl routes data but cannot analyze it.

LogZilla AI Example

```
# Prompt: "Generate security report"

LogZilla AI Response:
- Threat Detection: 847 DNS amplification attacks
- MITRE Mapping: T1110.001, T1498.002
- Remediation: Cisco ASA, Palo Alto commands

# In Cribl: Not possible. Routes data only.
```

LogZilla Does Everything Cribl Does (Plus More)

Multi-Destination Routing

LogZilla Forwarder supports multiple simultaneous destinations:

Data Transformation

LogZilla provides powerful transformation:

- **Syslog**: TCP/UDP to any receiver
- **Splunk HEC**: Direct HTTP Event Collector
- **SNMP Traps**: To any trap receiver
- **File**: JSON or TSV format

- **Rewrite Rules**: Match and modify fields
- **Lua Rules**: Complex parsing and enrichment
- **LogZilla Apps**: Packaged vendor parsing
- **Tag Enrichment**: Add context (site, role)

Bottom line: *There is no use case where Cribl is required. LogZilla provides routing, transformation, AND analysis in one platform.*

Key Value Propositions

Complete Platform
SIEM, SOAR, AI in one. No routing layer needed.

Built-in Deduplication
80-95% reduction eliminates Cribl use case.

Simpler Architecture
One product vs pipeline + destination.

Key Differentiators

Complete Platform

Cribl routes data but does not analyze it. LogZilla provides SIEM, SOAR, and AI capabilities in a single platform.

AI-Powered Analysis

LogZilla generates threat reports and remediation commands. Data routing tools provide no analysis capabilities.

Simplified Architecture

LogZilla's built-in deduplication eliminates the need for a separate data routing layer.

Single Platform Cost

LogZilla provides routing, analysis, and response in one product rather than requiring multiple tools.

Common Considerations

"Cribl reduces our Splunk costs"

LogZilla's deduplication achieves 80-95% reduction without sampling. Cribl sampling loses data permanently; LogZilla preserves full fidelity for forensics and compliance.

"Cribl is the industry standard"

Cribl solves a problem created by expensive SIEMs. LogZilla eliminates the problem entirely with efficient pricing and deduplication.

"We need multi-destination routing"

LogZilla Forwarder routes to syslog, Splunk HEC, SNMP, and file simultaneously. Same capability, plus analysis, in one product.

"We're already invested in Cribl"

LogZilla can replace both Cribl AND your destination SIEM, or complement existing infrastructure during migration.

Migration Path: Cribl + Splunk to LogZilla

Phase	Action	Duration	Outcome
1. Parallel Ingest	Send logs to both LogZilla and Cribl/Splunk	2-4 weeks	Validate LogZilla captures all data
2. Dashboard Migration	Recreate critical dashboards in LogZilla	1-2 weeks	Operational parity confirmed
3. Alert Migration	Move alerting rules to LogZilla triggers	1-2 weeks	Detection coverage validated
4. Cutover	Redirect sources to LogZilla, decommission Cribl	1 week	Single platform operational

Result: *Eliminate two products (Cribl + Splunk), reduce costs 60-80%, gain AI capabilities, preserve full data fidelity.*

ROI Summary

License Savings
Eliminate Cribl license + reduce/eliminate Splunk. Typical savings: 60-80%.

Operational Savings
One platform to manage vs two. Reduced complexity, fewer staff hours.

Capability Gains
AI analysis, SOAR automation, natural language queries not available with Cribl.

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