LOGZILLA

log intelligence for mission-critical networks
www.logzilla.net

SIEM Offload Economics

Reduce Splunk and SIEM Costs by 60-80%

60-80%
Volume Reduction

$3.7M
Annual Savings (5TB/day)

<1 sec
Query Speed

The Problem: SIEM Cost Explosion

Enterprise SIEMs charge based on data volume. As infrastructure grows, costs scale linearly while value does not.

Typical Splunk Pricing

Daily Ingest	Annual Cost
100 GB/day	$150K - $200K
500 GB/day	$500K - $750K
1 TB/day	$1.0M - $1.5M
5 TB/day	$4.0M - $6.0M

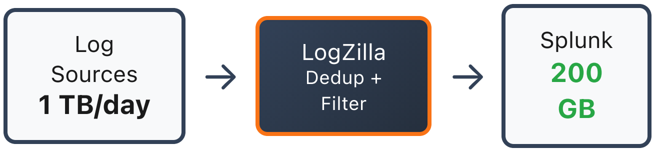
Licensing only. Add infrastructure, storage, and personnel.

Hidden Costs

- **Storage** – Hot/warm/cold tiers multiply costs
- **Rehydration** – Accessing archived data incurs fees
- **Personnel** – Splunk expertise commands premium salaries
- **Infrastructure** – Indexers, search heads, forwarders

The Solution: Intelligent Pre-Processing

LogZilla sits in front of the SIEM, reducing volume before expensive indexing.


Log Sources **1 TB/day** → LogZilla Dedup + Filter → Splunk **200 GB**

How LogZilla Reduces Volume

- **Deduplication** – Patented algorithm (US #8,775,584) collapses repeated events
- **Noise Filtering** – Non-actionable events filtered before forwarding
- **Actionable Forwarding** – Only security-relevant events reach SIEM
- **Full Archive** – All original data retained for compliance

Example: 10,000 identical alerts → 1 event with count of 10,000

Cost Reduction Scenarios

500 GB/day Environment

Before (Splunk)	$600K/yr
After (80% reduction)	$120K/yr
LogZilla License*	~$245K/yr
Net Cost	**$365K/yr**

$235K
Annual Savings (39%)

1 TB/day Environment

Before (Splunk)	$1.2M/yr
After (80% reduction)	$240K/yr
LogZilla License*	~$269K/yr
Net Cost	**$509K/yr**

$691K
Annual Savings (58%)

5 TB/day Environment

Before (Splunk)	$5.0M/yr
After (80% reduction)	$1.0M/yr
LogZilla License*	~$402K/yr
Net Cost	**$1.4M/yr**

$3.6M
Annual Savings (72%)

Volume Reduction (Dedup + Filtering)

Log Source	Dedup	Combined
Network Infrastructure	75-85%	**85-95%**
Firewalls	70-80%	**80-90%**
Windows Event Logs	60-70%	**70-85%**
Application Logs	65-75%	**75-85%**
Cloud Infrastructure	55-65%	**70-80%**
Security Events	30-50%	**50-70%**

**During event storms, reduction can exceed 99% (308K events → 4 forwarded).*

Why Deduplication Works

- Interface flapping: 10,000 events → 1 event
- Failed logins: 5,000 events → 1 per user
- Heartbeats: 86,400/day → 0 forwarded
- Status messages: Millions → 0 forwarded

LogZilla vs. Splunk Direct

Capability	LogZilla + Splunk	Splunk Only
Cost per TB/day	**$50-100K**	$1M+
Query Speed	**Sub-second**	Minutes
Deduplication	**Real-time, patented**	Post-ingest
Automation (SOAR)	**Built-in**	Add-on
AI Analysis	**Included (on-prem)**	Add-on
Air-Gap Support	**Yes**	Limited

Additional Value

- **Faster Queries** – Sub-second on billions of events
- **Real-Time Enrichment** – Device metadata, threat intel
- **Compliance Archive** – Full fidelity, instant search
- **Automation** – Fix issues before they reach Splunk

Proven Customer Results

- **Large Financial Services Firm** – Eliminated 4,000+ false positive tickets/week
- **Defense Cyber Operations Command** – Major Splunk cost savings via deduplication
- **Major Healthcare System** – Minutes to value vs 6 months; 90M daily events
- **Higher Education Institution** – 70% faster incident mgmt, 99% less response effort

**LogZilla pricing estimated and subject to change. Source: logzilla.net/case-studies*