LogZilla vs CrowdStrike: Product Comparison

Product Comparison | December 2025

Executive Summary

CrowdStrike excels at endpoint protection, but its **endpoint-centric focus, limited log management, and per-endpoint pricing** create gaps. LogZilla **complements CrowdStrike** by handling network, infrastructure, and application logs with AI analysis.

Summary: LogZilla complements CrowdStrike EDR by providing full log management, SIEM capabilities, and multi-vendor AI analysis for network and infrastructure.

Log Management: LogZilla Wins

Factor	LogZilla	CrowdStrike LogScale
Pricing	Events/day (predictable)	GB/day ingestion
Focus	Purpose-built logs	Acquired (Humio)
Deduplication	Yes (patented)	No
Storage	80-95% reduction	Standard compression

CrowdStrike Pain Points

- LogScale pricing scales with volume
- Endpoint-first, logs are secondary
- No deduplication = higher costs
- Per-endpoint pricing expensive at scale

SIEM/SOAR: LogZilla Wins on Value

Feature	LogZilla	CrowdStrike
SIEM	Built-in	Falcon add-on
SOAR	Built-in	Falcon Fusion (extra)
Log Sources	Any (vendor-neutral)	CrowdStrike-centric
Pricing	Predictable	Per-endpoint + modules

CrowdStrike Pain Points

- SIEM requires Falcon platform
- Best with CrowdStrike data
- SOAR requires Falcon Fusion
- Third-party logs are secondary

AI Capabilities: LogZilla Wins on Breadth

Capability	LogZilla	CrowdStrike Charlotte AI
Natural Language	Yes all log sources	Yes endpoint-focused
Network/Infrastructure	Full support	Limited
Multi-Vendor Remediation	Cisco, Juniper, Palo Alto, etc.	Endpoint-focused
Compliance Mapping	CIS, NIST, ISO, PCI-DSS	Endpoint compliance

Real-World AI Example: Security Operations

Prompt: "Generate a security incident report for the last 24 hours. Include threat detection across all log sources and vendor-specific remediation."

LogZilla AI Response (analyzing 13.6M events across all sources in seconds)

Threat Detection (All Sources)

Source	Finding	Severity
Firewall	DNS Amplification	Critical
SSH Servers	Brute Force	High
Network	Port Scanning	Medium

MITRE ATT&CK Mapping

Technique	Tactic	Evidence
T1110.001	Credential Access	12,453 SSH failures
T1498.002	Impact	DNS amplification
T1046	Discovery	Port scanning

AI-Generated Remediation

```
# Cisco ASA: Block attacker
access-list OUTSIDE_IN deny ip host 45.142.xxx.xxx any

# Palo Alto: Create threat block
set address "Threat-Actor-1" ip-netmask 45.142.xxx.xxx/32

# Linux: Fail2ban
fail2ban-client set sshd banip 45.142.xxx.xxx

# Juniper SRX: Security policy
set security policies policy block-threat then deny
```

Top Threat Sources

Source IP	Country	Action
45.142.xxx.xxx	Russia	Blocked
185.220.xxx.xxx	Germany	Blocked

Charlotte AI: *Excellent for endpoints, but no network device remediation commands.*

Complement Strategy: LogZilla + CrowdStrike

Component	Best Solution
Endpoint Protection	CrowdStrike EDR
Log Management	LogZilla (cost-effective)
Network/Infra SIEM	LogZilla (vendor-neutral)
Multi-Vendor AI	LogZilla (broader coverage)

Customer Benefits

- **Best of Both**: CrowdStrike EDR + LogZilla logs
- **Cost Savings**: Avoid LogScale for high-volume
- **AI Breadth**: Analysis across all sources
- **No Lock-In**: Vendor-neutral SIEM

Key Value Propositions

Complement, Not Replace

Keep CrowdStrike EDR. Add LogZilla for logs and network AI.

Multi-Vendor AI

Remediation for Cisco, Juniper, Palo Alto, Linux, Windows.

Cost-Effective Logs

80-95% storage reduction vs LogScale. Predictable pricing.

Key Differentiators

Complementary Solution

CrowdStrike excels at endpoint protection. LogZilla extends visibility to network, infrastructure, and application logs with AI-powered analysis.

Multi-Vendor Coverage

LogZilla AI provides remediation commands for Cisco, Juniper, Palo Alto, and other network vendors—beyond endpoint-focused tools.

Cost-Effective Log Management

LogZilla's patented deduplication provides 80-95% storage reduction compared to traditional log management solutions.

Unified Visibility

Correlate endpoint alerts with network and infrastructure logs for complete incident context.

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