LogZilla vs Exabeam: Product Comparison

Product Comparison | December 2025

Executive Summary

Exabeam is a SIEM focused on User and Entity Behavior Analytics (UEBA), but its **complexity, high cost, and narrow focus** create gaps. LogZilla delivers broader AI analysis with **simpler deployment and lower TCO**.

Simplicity: LogZilla Wins

Factor	LogZilla	Exabeam
Deployment	Minutes (Docker)	Weeks to months
Architecture	Single platform	Multiple components
Learning Curve	Hours	Extensive training
UEBA Tuning	AI ready immediately	Months of baselining

Exabeam Pain Points

- Complex deployment and configuration
- UEBA requires significant tuning
- Steep learning curve
- Dedicated expertise required

Cost: LogZilla Wins on TCO

Factor	LogZilla	Exabeam
Licensing	Events/day	Users + data volume
SOAR	Included	Separate product
AI/UEBA	Included	Core (premium)
Services	Minimal	Often required

Exabeam Pain Points

- Complex pricing model
- SOAR is additional cost
- Professional services often needed
- Training is expensive

AI Capabilities: LogZilla Wins on Breadth

Capability	LogZilla	Exabeam
Natural Language Queries	Yes plain English	No query syntax
Analysis Scope	SecOps, NetOps, InfraOps, AppOps, CloudOps	Security/UEBA focused
Remediation Commands	Vendor-specific CLI	Not available
MITRE ATT&CK	Automatic mapping	Manual tagging

Real-World AI Example: Privileged Access Audit

Prompt: "Generate a privileged access review. Include sudo/su operations, service account activity, and compliance mapping."

LogZilla AI Response (analyzing 13.6M events in 3.8 seconds)

Privileged Escalation Summary

Metric	Value	Compliance
sudo/su Operations	183	Justification required
Unique Privileged Users	12	SOX, PCI-DSS
Root Access Events	47	Review pending

User Behavior with Risk Scoring

User	Command	Risk	Status
kryskoy	su to root	85	PENDING
svc_backup	sudo su - root	72	PENDING
admin_jones	sudo /bin/bash	68	REVIEW

Compliance Framework Mapping

Framework	Control	Status
SOX-ITGC-04	Privileged Access	REVIEW
PCI-DSS 8.2	User Auth	PARTIAL
HIPAA 164.312	Access Controls	REVIEW

AI-Generated Remediation

```
# Session recording for privileged access
auditctl -a always,exit -F arch=b64 -S execve -F euid=0

# Require MFA for sudo
echo "auth required pam_google_authenticator.so" >>
/etc/pam.d/sudo
```

In Exabeam: *User timelines, but no compliance mapping or remediation.*

Log Management: LogZilla Wins

Feature	LogZilla	Exabeam
Performance	10TB/day single server	Varies
Deduplication	Yes (patented)	No
Storage	80-95% reduction	Standard
Query Speed	Sub-second	Varies

LogZilla + Exabeam (Complement)

For customers invested in Exabeam UEBA:

- **Log Management**: High-volume logs in LogZilla
- **Network/Infra**: Visibility Exabeam lacks
- **AI Breadth**: Natural language all domains
- **SOAR**: Built-in without separate product

Key Value Propositions

Broader AI Analysis

SecOps, NetOps, InfraOps, AppOps, CloudOps, Compliance.

Simpler Deployment

Minutes vs months. No UEBA tuning required.

Lower TCO

SOAR included. Predictable pricing. Less services.

Key Differentiators

Rapid Deployment

LogZilla deploys in minutes without the extended UEBA tuning period required by behavior analytics platforms.

Integrated Platform

SIEM, SOAR, and AI capabilities included in a single platform with predictable pricing.

Broader AI Coverage

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

Natural Language Interface

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

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