LogZilla Use Cases

Operational Intelligence for Every Environment

Key Capabilities: AI-powered analysis in seconds | 60-80% SIEM cost reduction | Sub-second queries on billions of events | Full air-gap support | Automated remediation

AI-Powered Operational Intelligence

The Problem: Traditional log analysis requires specialized query languages, manual correlation, and hours of investigation.

The Solution: Ask questions in plain English. AI analyzes billions of events, correlates across devices, and provides vendor-specific remediation commands in seconds.

Real-World NetOps Report

> Analyze network operations events from the last 2 hours and provide remediation steps.

Network Operations Incident Report

Events: 5.06M | Baseline: 3.90M (+29.6%)

Key Findings:

CRITICAL PKI Certificate Failure – 20+ Cisco devices
CRITICAL AD Connector DNS Failure – ISE nodes
HIGH Wireless Auth Failures – 92,734 events

Remediation (Cisco IOS):

```
crypto pki authenticate sdn-network-infra-iwan
crypto pki enroll sdn-network-infra-iwan
```

AI Provider Options

Provider	Best For
OpenAI / Anthropic	Cloud, maximum capability
Ollama (On-Prem)	Air-gap, data sovereignty
Scaleway	EU data residency

Real-World SecOps Report

> Generate a security incident report with MITRE ATT&CK mapping.

Security Operations Incident Report

Events: 448,698 | Threats: 4 Critical

Threat Intelligence:

CRITICAL DNS Amplification – 20+ cloud IPs
CRITICAL IP Spoofing – 13 attempts blocked
HIGH PKI Failures – 88 devices at risk

MITRE ATT&CK: T1498.002, T1599.001, T1110.004

Remediation (Firepower):

```
ip verify unicast source reachable-via rx
access-list OUTSIDE_IN deny ip host 198.51.x.x any
```

What Makes This Unique

- **Natural language** – No query language required
- **Millions of events in seconds** – Instant analysis
- **Cross-device correlation** – Automatic root cause
- **Vendor-specific commands** – Ready-to-use CLI
- **Works offline** – On-prem Ollama for air-gap

Use Case Summary

SIEM Cost Reduction

Problem: SIEM costs scale with data volume

Solution: 60-80% volume reduction via deduplication

Result: $1.2M → $509K annual savings

MTTR Acceleration

Problem: Hours/days to resolve incidents

Solution: AI analysis + automated remediation

Result: Hours → Seconds resolution

NOC Operations

Problem: Alert fatigue, 10K+ daily alerts

Solution: 95% noise reduction, enrichment

Result: 500 actionable alerts/day

SOC Operations

Problem: Threat detection takes hours

Solution: Real-time correlation, AI hunting

Result: 80% fewer false positives

Air-Gapped Networks

Problem: No AI in classified environments

Solution: On-prem Ollama, zero phone-home

Result: Full AI capability offline

Multi-Vendor

Problem: Weeks to parse new vendors

Solution: App Store with 20+ vendor packs

Result: Minutes to value

Accelerated Incident Response (MTTR)

Problem: Detection takes minutes, triage requires SSH to multiple devices, root cause analysis spans hours.

Solution: Real-time detection, AI-powered root cause in seconds, automated remediation with approval workflows.

Phase	Before	After
Detection	5-15 min	Real-time
Root Cause	Hours	Seconds
Remediation	15-60 min	Automatic
Total MTTR	**Hours/Days**	**Seconds/Min**

Business Impact

- **Reduced downtime** – Issues fixed before users notice
- **Lower staffing costs** – Automation handles routine tasks
- **Fewer escalations** – AI provides expert-level analysis
- **24/7 coverage** – Automation works around the clock

NOC & SOC Operations

Network Operations (NOC)

Problem: Alert fatigue from 10K+ daily alerts. Critical issues hide in noise.

Solution: 95% noise reduction, enrichment, real-time dashboards, automation.

Metric	Before	After
Daily Alerts	10,000+	500 actionable
Staff Efficiency	Reactive	Proactive

Security Operations (SOC)

Problem: Threat detection takes hours. Correlation across sources is manual.

Solution: Real-time correlation, AI threat hunting, built-in compliance reports.

Metric	Before	After
Threat Detection	Hours	Real-time
False Positives	High	80% reduction

Universal Log Support

The Problem

Enterprise networks include dozens of vendors. Each generates different log formats. Traditional tools require weeks of custom parsing for each new source.

The Solution

LogZilla accepts ALL log data – any device that sends syslog, any API, any file format. No parsing required to start seeing value.

- **Universal ingest** – Syslog, API, file, SNMP traps
- **Instant visibility** – Search and alert on any event immediately
- **App Store** – One-click install of dashboards, rules, and triggers
- **Enrichment** – Add context from CMDB, topology, threat intel

App Store Advantage

Pre-built modules provide instant dashboards, custom rules, triggers, and AI prompts for popular vendors:

40+ App Store Modules

Network

- Cisco (IOS, ASA, ISE, Meraki, Nexus, WLC, Firepower)
- Palo Alto Networks
- Fortinet FortiGate
- Juniper JunOS
- Check Point
- SonicWall
- WatchGuard
- Ubiquiti UniFi

Security

- CylancePROTECT
- FireEye
- Trend Micro
- Symantec EPM
- McAfee MWG
- Snort / Zeek
- Fail2ban

Infrastructure

- Windows / Linux
- VMware vSphere
- AWS / Azure / GCP
- Kubernetes
- Infoblox DNS
- Nginx / Postfix
- Microsoft MFA

App Store modules are optional enhancements. LogZilla works with ANY log source out of the box.

Additional Use Cases

Compliance & Audit

Retention policies, tamper-evident storage, RBAC, PCI/HIPAA/SOX reports

Result: Audit prep: Weeks → Hours

DevOps

Real-time ingest, CI/CD integration, sub-second search on billions

Result: Debug: Hours → Minutes

IoT & OT

10 TB/day, SNMP/syslog/API, ICS parsers, air-gap ready

Result: Full telemetry visibility

MSP Multi-Tenant

Customer separation, white-label, SLA reporting

Result: Improved margins

Air-Gapped

Zero phone-home, on-prem AI, offline updates

Result: Full capability offline

Executive Reporting

Business impact, trends, risk dashboards, AI insights

Result: Data-driven decisions

SIEM Cost Reduction (60-80% Savings)

Problem: SIEM costs scale with data volume—often $1M+ annually for 1TB/day.

Solution: LogZilla reduces volume before expensive SIEM indexing via patented deduplication, noise filtering, and actionable forwarding.

Metric	Before	After
Daily Ingest	1 TB/day	200 GB/day
Splunk License	$1.2M/year	$240K/year
LogZilla License	—	$269K/year
Net Savings	**$691K/year (58%)**	

Volume Reduction by Source

Log Source	Typical Reduction
Network (Cisco, Juniper)	85-95%
Firewalls (Palo Alto, Fortinet)	80-90%
Windows / Application	70-85%
Cloud (AWS, Azure)	70-80%

During event storms, reduction can exceed 99%

Proven Customer Results

Industry	Challenge	Result
Financial Services	Alert fatigue overwhelming SOC	Eliminated 4,000+ false positive tickets per week
Defense/Federal	Splunk costs unsustainable	Major cost savings through deduplication
Healthcare	Slow deployment, 90M events/day	Minutes to value vs 6 months with competitors
Higher Education	Slow incident response	70% faster management, 99% less response effort
Technology	Complex root cause analysis	AI-powered instant root cause identification

Technical Specifications

Capability	Specification
Ingest Rate	10+ TB/day per server
Query Speed	Sub-second on billions
Deduplication	Patented (US #8,775,584)
AI Providers	OpenAI, Anthropic, Ollama, Scaleway
Context Window	Per model/provider

Deployment	Options
Cloud	SaaS, AWS, Azure, GCP
On-Premises	VM, bare metal, Docker
Air-Gap	Full offline capability
Appliance	Pelican case, 2U rack
Licensing	Subscription or perpetual

Next Steps

1. **Identify** primary use case(s) for your environment
2. **Schedule** discovery call to assess requirements
3. **Deploy** POC to validate value (typically 2-4 weeks)
4. **Measure** outcomes against baseline

Typical POC Timeline: 2-4 weeks from kickoff to results

Why LogZilla?

- AI analysis in seconds, not hours
- 60-80% SIEM cost reduction
- Sub-second queries on billions of events
- Patented deduplication technology
- Full air-gap and on-prem AI capability
- 20+ vendor parsers out of the box