Tactical AI Log Intelligence for Defense Ops

Air-Gapped • On-Prem AI • Zero Phone-Home

Mission-Ready Operational Intelligence

LogZilla delivers AI-powered operational intelligence for air-gapped and contested environments. On-prem AI analyzes billions of events in seconds with zero external dependencies. Purpose-built for FOB, expeditionary, and shipboard operations where connectivity is denied or degraded.

10TB+	80-95%	<3 sec
Events/Day Single Node	Data Reduction	AI Query Response

Deploy Fast

LogZilla deploys as a Pelican-case appliance, VM, or air-gapped server. Purpose-built for FOB and expeditionary ops. From first ingest, events are deduplicated, enriched, and correlated into actionable intelligence.

Deployment Options

Ruggedized appliance, virtual machine, Docker/Kubernetes, or bare metal. Operational in under 30 minutes.

Mission-Ready

LogZilla operates fully offline with on-prem AI. Detect threats and respond faster in denied networks.

Do More With Less

LogZilla collapses duplicate events and filters noise so undermanned teams maintain situational awareness without additional personnel.

Capability Matrix

Capability	Status
Air-Gapped Operation	Full Support
On-Prem AI/LLM	No Cloud Required
SIEM Functions	Built-in
SOAR Automation	Built-in
Patented Deduplication	US #8,775,584
Multi-Vendor Support	500+ Sources
Real-Time Alerting	Sub-Second
Compliance Reporting	NIST/DISA STIG

Zero Phone-Home Architecture
All processing occurs locally. No telemetry, no license callbacks, no external dependencies. Designed for SCIF and classified environments.

Supported Platforms

Network
Cisco, Juniper, Palo Alto, Fortinet, Arista

Security
Firewalls, IDS/IPS, EDR, NAC

Infrastructure
Windows, Linux, VMware, Storage

Applications
Web servers, databases, custom apps

AI-Powered Operational Intelligence

Natural Language Queries • Automated Analysis • Vendor-Specific Remediation

On-Premises AI That Understands Your Mission

Ask questions in plain English. LogZilla AI analyzes millions of events and returns actionable intelligence with device-specific remediation commands. No cloud connectivity required. No data leaves your network.

AI Analysis Domains

Domain	Capabilities
SecOps	Threat detection, IOC extraction, MITRE ATT&CK mapping
NetOps	Topology impact, cascading failures, device CLI
InfraOps	Risk assessment, outage prediction, capacity
Compliance	NIST 800-53, DISA STIG, RMF evidence collection

Example AI Interaction

Operator Query:
"Generate a security incident report for the last 2 hours with threat prioritization"

LogZilla AI Response (analyzing 8.6B events in 2.1 seconds):

Priority	Threat	Confidence	Events
CRITICAL	DNS Amplification Attack	95%	20+
CRITICAL	IP Spoofing (Botnet)	90%	13
HIGH	PKI Cert Renewal Failure	85%	176
HIGH	Spanning Tree Instability	70%	44

AI-Generated Remediation

Vendor-specific commands generated automatically:

```
# Infoblox: Enable DNS Response Rate Limiting
set rrl enable
set rrl responses-per-second 5

# Cisco FTD: Verify uRPF for IP spoofing
show running-config interface | include urpf

# Cisco Switch: PKI certificate renewal
crypto pki authenticate sdn-network-infra-iwan
crypto pki enroll sdn-network-infra-iwan

# Spanning Tree: Identify rogue device
show mac address-table interface Gi1/0/24
show spanning-tree interface Gi1/0/24 detail
```

Automated Response (SOAR)

Event-Triggered Automation

Execute remediation scripts on pattern match. Auto-recover interfaces, block threats, restart services.

Event Correlation

Detect flapping, brute force, and multi-stage attacks. Threshold-based escalation with suppression.

Compliance Framework Support

NIST 800-53
Full control mapping and evidence

DISA STIG
Automated compliance checks

RMF
Continuous monitoring support

Deployment Options & Integration

Flexible Deployment • Existing SIEM Integration • Rapid Time-to-Value

Deployment Configurations

Option	Use Case	Capacity
Pelican Appliance	FOB, expeditionary, mobile command	10TB/day
Rack Server	Data center, shipboard, secure facility	10TB/day
Virtual Machine	Existing infrastructure (tuned hypervisor)	1TB/day
Kubernetes	Cloud-native, massive scale	230TB/day

Pelican/Rack: RTX Pro 6000 Blackwell (96GB), Graid T1010, 512GB DDR5 ECC, on-prem AI.

Extend SIEM Investment

Deployed in front of Splunk or QRadar, LogZilla deduplicates and filters events before expensive storage, cutting volume 60-80%. Forward only actionable data to existing SIEM infrastructure.

SIEM Forwarding Options

Syslog:

TCP/UDP to any receiver

Splunk HEC:

Direct HTTP Event Collector

SNMP Traps:

To any trap receiver

File:

JSON or TSV format

Integration Architecture

Typical Defense Deployment:
Network devices → LogZilla (dedupe/enrich/analyze) → Existing SIEM (reduced volume) + Local retention (full fidelity)

Predator Appliance Specs

Component	Specification
CPU	AMD EPYC 9354 (32-core, 3.25GHz)
RAM	512 GB DDR5 5600MHz ECC
GPU	RTX Pro 6000 Blackwell (96GB)
Storage	Graid T1010 + 16x 7.68TB NVMe
Network	2x 1GbE + 2x 10GbE

Graid T1010: *GPU-accelerated NVMe RAID delivering 110GB/s throughput, 19M IOPS, and 50x faster rebuild than traditional RAID.* graidtech.com

Situational Awareness

LogZilla enriches events with topology, location, and mission context so operators see root cause and impact, not cryptic log streams.

Event Enrichment

Automatic tagging with site, role, criticality, and mission assignment. Correlate events across disparate systems.

Visual Dashboards

Real-time operational views with drill-down capability. Dark theme available for tactical operations centers.

Support & Training

Service	Included
24/7 Support	Yes
On-Site Training	Available
Custom Integration	Available
Documentation	Full Access

Prove It On Your Data

Book a 30-minute demo or request a proof-of-concept deployment.
See LogZilla process your actual log data in a secure environment.