

# Air-Gap and AI Security Brief

DEFENSE

On-Premises AI for Classified and Contested Environments

LogZilla provides full operational intelligence capabilities in completely air-gapped environments. The platform includes on-premises AI using Ollama, requiring no external API calls, cloud connectivity, or phone-home functions.

## Air-Gap Architecture

### Zero External Dependencies

- **No license server calls** – Licensing is file-based
- **No telemetry** – Zero usage data transmitted externally
- **No update checks** – Manual update packages available
- **No cloud AI** – On-premises Ollama handles all AI functions

### Network Isolation Modes

Mode	Description	Connectivity
Full Air-Gap	No external network	None
Partial Air-Gap	Internal network only	LAN only
Secure Enclave	Limited external via proxy	Controlled egress

## On-Premises AI

### Ollama Integration

- **Model** – Llama, Mistral, or other Ollama-supported models
- **Location** – Runs locally on LogZilla server or dedicated GPU node
- **Data** – All queries and responses remain on-premises
- **Performance** – GPU acceleration recommended

AI Provider Settings:  
└─ External (OpenAI/Anthropic) - Disabled  
└─ Internal Ollama - Enabled  
|   └─ Base URL: http://localhost:11434  
|   └─ Model: llama, mistral, mixtral, etc.  
└─ Disabled - AI features off

## Compliance Alignment

Framework	Relevant Controls
NIST 800-53	SC-7, SC-8 (Boundary/Transmission)
CMMC 2.0	Level 2/3 for CUI handling
ITAR	No foreign data processing

## Security Controls

### Data Sovereignty

- All log data remains on-premises
- AI processing occurs locally
- No data replication to external systems
- Full control over data retention and destruction

### Access Controls

- Role-based access control (RBAC)
- LDAP/Active Directory integration (internal)
- Local user management for isolated networks
- Audit logging of all administrative actions

### Encryption

- TLS for all internal communications
- Encryption at rest (configurable)
- Certificate management for air-gapped PKI

## Deployment Scenarios

Scenario	Description	Form Factor
Classified Network	Full air-gap, no external connectivity	Rack or VM
Forward Operating Base	Tactical deployment, expeditionary	Pelican Case
Shipboard	Naval vessel, isolated network	Rack Mount
Mobile Command	Vehicle-mounted operations	Pelican Case
SCIF	Secure compartmented facility	Rack or VM

See Defense Appliance Specification for detailed hardware configurations.

NATO STANAG      Information security requirements

Swedish Military      FMV security requirements

## Frequently Asked Questions

**Q: Can LogZilla function without internet?**

A: Yes. All features including AI work without external connectivity.

**Q: Does AI require cloud processing?**

A: No. On-premises Ollama handles all AI. No external calls.

## Update & Maintenance

### Offline Updates

- Download update package on connected system
- Verify checksums and signatures
- Transfer via approved media (USB, optical)
- Apply using local package manager

### AI Model Updates

- Model weights versioned and transferable
- Rollback capability if needed
- No external connectivity required

### Support Options

- On-site support with cleared personnel
- Secure documentation portal
- Offline knowledge base included

## Hardware Options

Component	Predator Appliance
CPU	AMD EPYC 9354 (32-core)
RAM	512 GB DDR5 ECC
GPU	RTX Pro 6000 Blackwell (96GB)
Storage	Graid T1010 (61TB usable)
Form Factor	Pelican Case or 2U Rack

See Defense Appliance Specification for full details.

### Key Takeaways

- Complete air-gap operation
- On-premises AI (no cloud dependencies)
- Zero phone-home functionality
- Tactical appliance available
- Proven in defense deployments