LOGZILLA

Federal Edition

LogZilla for Federal Agencies

NIST-Aligned Log Intelligence for Civilian and Defense Missions

NIST	Air-Gap	On-Prem	Zero
800-53 Aligned	Capable	AI Included	Phone-Home

The Federal Challenge

Mission-Critical Security Requirements:

- **Compliance mandates**: FISMA, NIST 800-53
- **Zero Trust architecture**: EO 14028 requirements
- **Air-gapped networks**: Classified environments
- **CDM integration**: DHS dashboard feeds
- **Budget constraints**: Do more with less

The AI Advantage

Federal-Ready Intelligence:

- **On-prem AI**: No cloud dependency
- **NIST alignment**: AU family controls
- **Threat hunting**: APT detection
- **Audit automation**: IG-ready reports
- **CDM feeds**: Dashboard integration

NIST 800-53 AU Family Coverage

Control	Description	Status
AU-2	Event Logging	Supports
AU-3	Content of Audit Records	Supports
AU-4	Audit Log Storage	Supports
AU-5	Response to Failures	Supports
AU-6	Audit Record Review	AI-Enhanced
AU-7	Audit Record Reduction	Patented
AU-9	Protection of Audit Info	Supports
AU-12	Audit Record Generation	Supports

Zero Trust Support: LogZilla provides continuous monitoring and verification aligned with EO 14028 and CISA Zero Trust Maturity Model requirements.

AI-Powered Threat Detection

SOC Analyst prompt: "Analyze all authentication events for indicators of APT activity in the last 24 hours."

```
ADVANCED THREAT ANALYSIS
Period: Last 24 Hours | Events: 2.4B | Systems: 12,847
═══════════════════════════════════════

THREAT INDICATORS DETECTED:

1. CREDENTIAL HARVESTING ATTEMPT
   Source: 185.xxx.xxx.xxx (Known APT Infrastructure)
   Target: VPN Gateway (vpn-east-01)
   Technique: T1110.003 (Password Spraying)
   Events: 847 failed attempts across 23 accounts
   Status: BLOCKED - Accounts locked

2. LATERAL MOVEMENT PATTERN
   Source: WS-FINANCE-047 (Internal)
   Activity: Unusual SMB enumeration
   Targets: 47 file servers in 2 hours
   Technique: T1021.002 (SMB/Windows Admin Shares)
   Status: INVESTIGATING - Isolated pending review

MITRE ATT&CK MAPPING:
  Initial Access: T1078 (Valid Accounts)
  Execution: T1059.001 (PowerShell)
  Persistence: T1053.005 (Scheduled Task)
  Lateral Movement: T1021.002 (SMB)
```

AI Use Cases for Federal

Use Case	Traditional	With AI
APT threat hunt	Days-Weeks	**Minutes**
FISMA audit evidence	Weeks	**Minutes**
Incident response	Hours	**Seconds**
CDM dashboard feeds	Manual	**Automated**
IG audit prep	Months	**Days**

Compliance Frameworks

- **FISMA**: Continuous monitoring support
- **CMMC**: DoD contractor requirements
- **CJIS**: Law enforcement data protection

Air-Gapped Deployment

Classified Environment Support:

- **Zero phone-home**: No external connections
- **On-prem AI**: Local LLM (Ollama)
- **Offline updates**: Air-gap transfer procedures
- **STIG-ready**: Hardened configuration

```
DEPLOYMENT OPTIONS
─────────────────────────────────────────

APPLIANCE (Ruggedized)
  Form Factor: 1U/2U Rackmount or Pelican Case
  Capacity: 10 TB/day single node
  AI: On-board GPU for local inference

VIRTUAL MACHINE
  Hypervisor: VMware, Hyper-V, KVM
  Resources: 16+ cores, 64GB+ RAM
  Storage: NVMe recommended

KUBERNETES
  Scale: 230+ TB/day
  HA: Multi-node clustering
  Storage: Persistent volumes
```

CDM Integration

```
CDM DASHBOARD FEED EXAMPLE
──────────────────────────────────────────

Agency: Example Agency
Feed Type: Security Event Summary
Period: Last 24 Hours

HWAM (Hardware Asset Management):
  Total Devices: 12,847
  Compliant: 12,341 (96.1%)
  Non-Compliant: 506

SWAM (Software Asset Management):
  Authorized Software: 847 titles
  Unauthorized Detected: 23 instances
  Remediation: In Progress

VUL (Vulnerability Management):
  Critical: 12 (SLA: 15 days)
  High: 47 (SLA: 30 days)
  Medium: 234 (SLA: 90 days)

TRUST (Boundary Protection):
  Blocked Connections: 847,293
  Allowed: 12.4M
  Anomalies: 3 (investigated)
```

Deployment Options

On-Premises

- Agency data center
- Full data sovereignty
- Air-gap capable
- STIG-hardened

Government Cloud

- AWS GovCloud
- Azure Government
- Authorized CSPs
- IL4/IL5 options

Hybrid

- Sensitive data on-prem
- Analytics in cloud
- Encrypted transport
- Flexible architecture

Why Federal Agencies Choose LogZilla

Metric	Improvement
FISMA audit prep	90% faster
Threat detection	Real-time
SIEM costs	70-90% savings
Analyst productivity	5x increase

Federal-Specific Benefits:

- **Mission-ready**: Air-gap and classified support
- **Compliant**: NIST 800-53, FISMA aligned
- **Sovereign**: On-prem AI, zero phone-home
- **Efficient**: Reduce costs, improve security

Mission-ready log intelligence for federal operations.

sales@logzilla.net | www.logzilla.net