LogZilla for Manufacturing

OT/IT Convergence Visibility Without Operational Impact

OT/IT	Zero	ICS/SCADA	AI
Unified Visibility	Production Impact	Log Collection	Copilot Included

The Manufacturing Challenge

OT/IT Convergence Complexity:

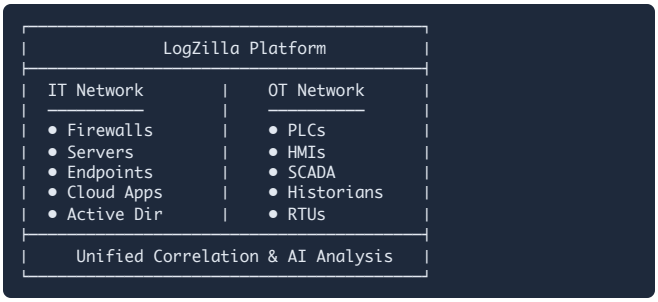
- **Visibility gaps**: OT systems invisible to IT security
- **Uptime requirements**: 24/7 production cannot stop
- **Legacy systems**: Decades-old PLCs and HMIs
- **Ransomware targets**: Manufacturing is #1 target
- **Supply chain pressure**: Downtime costs millions

The AI Advantage

Manufacturing-Aware Intelligence:

- **Passive collection**: No impact on production
- **OT protocol support**: Modbus, DNP3, EtherNet/IP
- **Anomaly detection**: Baseline deviation alerts
- **Downtime prevention**: Predictive maintenance
- **IT/OT correlation**: Unified threat view

OT/IT Convergence Architecture



Passive Collection: LogZilla receives logs via syslog, SNMP, and API without active scanning or polling that could disrupt production systems.

AI-Powered OT Security Monitoring

OT Security Analyst prompt: "Show all anomalies in the production network for the last 24 hours with safety impact assessment."

```
OT SECURITY ANALYSIS
Period: Last 24 Hours | PLCs: 847 | Events: 12.4M
═══════════════════════════════════════════════

PRODUCTION STATUS: NORMAL (99.7% uptime)

⚠ ANOMALIES DETECTED: 3

1. UNAUTHORIZED ACCESS ATTEMPT
   Target: HMI-PAINT-LINE-03
   Source: Engineering workstation (WS-ENG-047)
   User: contractor_jsmith
   Time: 02:14 AM (outside maintenance window)
   Status: BLOCKED - Credentials revoked

2. FIRMWARE CHANGE DETECTED
   Device: PLC-ASSEMBLY-12 (Allen-Bradley)
   Change: Logic modification
   User: plc_admin
   Status: VERIFIED - Scheduled maintenance

3. NETWORK BASELINE DEVIATION
   Segment: Welding Cell 7
   Traffic: +340% vs 7-day baseline
   Cause: New robot programming upload
   Status: VERIFIED - Expected activity

SAFETY SYSTEMS: ALL NORMAL
  E-Stops: 47/47 | Safety PLCs: 12/12 | Fire: Online
```

AI Use Cases for Manufacturing

Use Case	Traditional	With AI
OT anomaly detection	Manual review	**Real-time**
Downtime root cause	Hours	**Minutes**
Compliance audit	Weeks	**Minutes**
Vendor access review	Manual	**Automated**
Safety system monitoring	Periodic	**Continuous**

Log Sources

- **OT Systems**: PLCs, HMIs, SCADA, historians
- **IT Systems**: Firewalls, servers, endpoints
- **Protocols**: Syslog, SNMP, API, files
- **MES/ERP**: Any system generating logs

Downtime Prevention and Root Cause Analysis

Production Manager prompt: "Analyze the unplanned downtime on Assembly Line 3 yesterday and identify root cause."

```
DOWNTIME ANALYSIS: ASSEMBLY LINE 3
Incident: Dec 3, 2024 14:23-15:47 (84 min)
Production Loss: 847 units ($423,500)
═══════════════════════════════════════

ROOT CAUSE IDENTIFIED: Network switch failure

TIMELINE:
  14:21:03 - Switch SW-PROD-07: CPU 98% (warning)
  14:22:47 - Switch SW-PROD-07: Memory exhausted
  14:23:01 - Switch failure - OT segment isolated
  14:23:02 - PLCs lost communication (12 devices)
  14:23:15 - Safety system triggered line stop
  14:45:00 - IT notified (22 min delay)
  15:12:00 - Backup switch installed
  15:47:00 - Production resumed

CONTRIBUTING FACTORS:
  - Switch firmware outdated (2019)
  - No redundant switch in segment
  - Monitoring gap (OT switch not in IT tools)

RECOMMENDATIONS:
  1. Deploy redundant switches in OT segments
  2. Add OT network devices to LogZilla monitoring
  3. Update firmware during next maintenance window
```

Supply Chain Security

```
VENDOR ACCESS AUDIT
Period: Last 30 Days | Vendors: 23
═══════════════════════════════════════

Vendor              | Sessions | Systems  | Risk
--------------------|----------|----------|------
Rockwell Support    | 12       | PLCs     | Low
Siemens Service     | 8        | HMIs     | Low
HVAC Contractor     | 47       | BMS      | Med ⚠
Robot Integrator    | 23       | Cells    | Low

⚠ HVAC CONTRACTOR REVIEW:
  - 47 sessions (3x normal)
  - Accessed 12 systems (expected: 4)
  - After-hours access: 8 sessions
  Recommendation: Scope review needed
```

Compliance Frameworks

Framework	Coverage
IEC 62443	Zone Monitoring
NIST CSF	Supports
ISO 27001	Audit Trails
FDA 21 CFR Part 11	Pharma/Food
IATF 16949	Automotive

Deployment Options

On-Premises

- Plant data center
- Air-gap capable
- Full data control
- No cloud dependency

Multi-Plant

- Central correlation
- Plant-level collectors
- Encrypted transport
- Global visibility

Hybrid

- OT data on-prem
- IT data in cloud
- Unified analytics
- Flexible architecture

Why Manufacturers Choose LogZilla

Metric	Improvement
OT visibility	100% coverage
Downtime root cause	85% faster
Vendor access audit	Automated
Compliance evidence	Continuous

Manufacturing-Specific Benefits:

- **Zero impact**: Passive collection only
- **Uptime protection**: Predictive alerts
- **OT/IT unified**: Single pane of glass
- **Supply chain**: Vendor access visibility

Protect production, unify OT/IT, prevent downtime.

sales@logzilla.net | www.logzilla.net