LogZilla for MSPs and MSSPs

Scale Your Managed Services with AI-Powered Operational Intelligence

5 min	Minutes	Billions	AI
Weekly Reports (vs. Hours)	Root Cause (vs. Days)	Events Analyzed Daily	Copilot Included

The MSP/MSSP Challenge

Traditional Approach Problems:

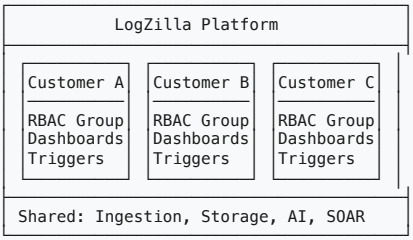
- **Weekly report prep takes hours**: Senior analysts tied up
- **Skilled labor shortage**: Experts stretched thin
- **Separate instances**: Per-customer infrastructure
- **Alert fatigue**: Millions of events daily
- **Manual correlation**: Hours per incident

The AI Advantage

Minutes Instead of Days:

- **Weekly reports in 5 minutes**: AI generates executive summaries
- **Junior staff empowered**: AI handles complexity
- **Cross-customer analysis**: Threat hunt all accounts
- **Vendor CLI commands**: Remediation included
- **Compliance reports**: PCI, HIPAA, CMMC ready

Multi-Tenant Architecture



RBAC Host Filtering

```
Customer A: 192.168.1.*, *.customerA.com
Customer B: 10.0.0.*, *.customerB.net
MSP Admin:  * (all customers)
```

Operational Efficiency Comparison

Before LogZilla

Customer	Infrastructure	Monthly Hours
Customer A	Dedicated SIEM	20 hours
Customer B	Dedicated SIEM	20 hours
Customer C	Dedicated SIEM	20 hours
Total	**3 instances**	**60 hours**

After LogZilla

Customer	Infrastructure	Monthly Hours
Customer A	Shared platform	5 hours
Customer B	Shared platform	5 hours
Customer C	Shared platform	5 hours
Total	**1 instance**	**15 hours**

AI-Powered Weekly Customer Reports

Analyst prompt: "Generate a weekly executive report for Acme Manufacturing covering security, infrastructure, and cost optimization."

```
WEEKLY EXECUTIVE REPORT: ACME MANUFACTURING
Period: Nov 25 - Dec 1 | Events: 1.2B | Generated: 5 min

EXECUTIVE SUMMARY
─────────────────────────────────────────────────

Health Score: 94/100 (↑2 from last week)
Threats Blocked: 847 | Uptime: 99.97%

SECURITY POSTURE
| Threat Type       | Attempts | Blocked | MITRE     |
|-------------------|----------|---------|-----------|
| Brute Force       | 412      | 412     | T1110.001 |
| Phishing          | 287      | 287     | T1566.001 |
| Priv Escalation   | 8        | 8       | T1078.002 |

COST OPTIMIZATION IDENTIFIED: $12,400/month
- Over-provisioned SQL DTUs: $4,200
- Unattached Azure Disks: $1,800
- Reserved Instance Mismatch: $6,400
```

AI Use Cases for MSPs

Use Case	Traditional	With AI
Weekly Executive Report	2-4 hours	**5 min**
Incident Root Cause	2-4 hours	**30 sec**
Compliance Audit Prep	1-2 weeks	**1 hour**
Cross-Customer Threat Hunt	Not feasible	**Real-time**
Cost Optimization Report	1 day	**2 min**

Value Delivered

- **Analyst time savings**: 80%+ reduction
- **Customer satisfaction**: Data-driven QBRs
- **Upsell opportunities**: AI finds issues
- **Competitive edge**: Capabilities others lack

MSSP Security Operations: Real-Time Threat Analysis

Analyst prompt: "Show critical security events across all customers in the last hour."

```
MSSP SECURITY SUMMARY
Customers: 47 | Events: 13.7M | Threats: 12

ACTIVE ATTACK: ACME MANUFACTURING
─────────────────────────────────────────────────

Coordinated brute force from 4 source IPs:
  34.89.212.6 (Germany) → Azure AD
  175.144.22.141 (Malaysia) → Azure AD
  86.205.25.195 (France) → Azure AD

REMEDIATION COMMANDS:
az network nsg rule create \
  --resource-group acme-prod-rg \
  --name BlockBruteForce \
  --access Deny \
  --source-address-prefixes 34.89.212.6 ...
```

Incident Report Generation

```
INCIDENT REPORT: DELTA LOGISTICS
Time: Last 2 Hours | Events: 6.65M

ROOT CAUSE ANALYSIS
─────────────────────────────────────────────────

Primary Issue: WLC auth storm
Affected Users: 847 accounts
Failure Types:
  - Invalid Password: 67%
  - EAP Abandoned: 22%
  - Client Timeout: 11%

Cross-Device Correlation:
  ISE Node: +79% load increase
  AD Connector: DNS SRV failures

REMEDIATION:
1. Fix AD connector config
2. Restart ISE services
3. Contact affected users
```

Deployment Options

Cloud (SaaS)

- logzilla.cloud managed
- Per-customer subdomains
- No infrastructure to manage
- Instant provisioning

Self-Hosted

- Single server: 10 TB/day
- Kubernetes: 10B+ events/day
- Your data center
- Full data control

Hybrid

- Central LogZilla instance
- On-prem collectors at sites
- Encrypted forwarding
- Best of both worlds

MSP-Friendly Licensing

Model	Description	Best For
Aggregate Volume	Total daily volume	Predictable pricing
Per-Customer Tiers	Volume bands	Variable sizes
Unlimited	Fixed price	Large MSSPs

No Hidden Fees:

- **No per-seat fees**: Add users freely
- **No per-device fees**: Unlimited endpoints
- **Predictable costs**: Budget on volume
- **Your margins**: Your pricing model

MSP Infrastructure Monitoring

Analyst prompt: "Analyze our hosting infrastructure health. Include cost anomalies."

```
MSP INFRASTRUCTURE ANALYSIS
Regions: US-East, US-West, EU-West | Events: 2.1M

COST ANOMALIES DETECTED
_____________________________________________
| Service     | Region  | Spike  | Impact     |
|-------------|---------|--------|------------|
| Lambda      | US-East | +311%  | $42,037/mo |
| Cosmos DB   | EU-West | +210%  | $8,400/mo  |
| Egress      | US-West | +156%  | $3,200/mo  |

Recommendation: Set Lambda concurrency limits
Command: aws lambda put-function-concurrency \
  --reserved-concurrent-executions 10
```

Why MSPs/MSSPs Choose LogZilla

- **AI-powered reports**: Minutes, not hours
- **Junior staff empowered**: AI handles complexity
- **Multi-tenant by design**: Built in, not bolted on
- **Margin improvement**: Shared infra, per-customer billing
- **Competitive edge**: Capabilities others lack

Success Metrics

Metric	Improvement
Weekly report generation	95% faster
Incident analysis	95% faster
Infrastructure consolidation	70-90%
Analyst productivity	5x increase

Integration Ecosystem

Ticketing & ITSM

- ServiceNow
- Jira Service Management
- Any REST API endpoint
- Custom webhooks

SOAR & Automation

- Built-in SOAR engine
- Script execution
- Webhook integration
- Event correlation (SEC)

Data Forwarding

- Splunk HEC
- Syslog (TCP/UDP/TLS)
- SNMP traps
- File export

Compliance Frameworks Supported

Framework	Coverage
PCI-DSS	Requirement 10 (audit trails)
HIPAA	Audit controls, log integrity
SOC 2	Logging and monitoring controls
CMMC	Audit and accountability
NIST 800-53	AU family controls

Compliance Benefits:

- **Immutable logs**: Tamper-proof audit trails
- **Retention policies**: Meet regulatory requirements
- **AI-generated evidence**: Audit-ready reports
- **Role-based access**: Segregation of duties

Getting Started

Phase 1: Pilot
Week 1-2

- Deploy LogZilla
- Onboard 2-3 customers
- Configure RBAC
- Validate isolation

Phase 2: Migration
Week 3-4

- Migrate remaining customers
- Deploy vendor parsers
- Configure automation
- Train NOC/SOC staff

Phase 3: Optimize
Ongoing

- Tune deduplication
- Build dashboards
- Automate reports
- Expand AI usage