LOGZILLA

Education Edition

LogZilla for Education

Protect Student Data, Secure Campus Networks, Enable Research

FERPA
Compliance Ready

80-95%
Data Reduction

Multi-Campus
Consolidation

AI
Copilot Included

The Education Challenge

Unique Campus Security Needs:

- **FERPA compliance**: Student record protection required
- **Open networks**: BYOD, guest access, research needs
- **Limited budgets**: Do more with less
- **Multi-campus**: Distributed IT, central visibility
- **Ransomware targets**: Education is high-value target

The AI Advantage

Education-Aware Intelligence:

- **Student data protection**: FERPA audit trails
- **Network visibility**: Campus-wide monitoring
- **Threat detection**: Ransomware early warning
- **Research support**: HPC and lab monitoring
- **Budget-friendly**: Reduce SIEM costs 70-90%

FERPA Compliance Support

Requirement	LogZilla Capability
Access Controls	RBAC
Audit Trails	Complete Logging
Data Integrity	Immutable Logs
Breach Detection	Real-time Alerts
Incident Response	AI-Powered

Multi-Campus Architecture: LogZilla consolidates logs from all campuses into a single searchable platform while maintaining RBAC separation between institutions.

Log Sources

- **Applications**: Syslog, SNMP, API, files
- **Identity**: LDAP, SAML, SSO providers
- **Network**: Firewalls, switches, wireless
- **Servers**: Linux, Windows, cloud instances

AI-Powered Campus Security

Security Analyst prompt: "Show all security incidents across all campuses in the last 24 hours with student data impact assessment."

```
CAMPUS SECURITY SUMMARY
Period: Last 24 Hours | Campuses: 5 | Events: 847M
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
Campus          | Events  | Incidents | Student Impact
----------------|---------|-----------|---------------
Main Campus     | 412M    | 3         | None
North Campus    | 187M    | 1         | None
Medical School  | 156M    | 2         | Under Review
Research Park   | 67M     | 0         | None
Online Division | 25M     | 1         | None

⚠️ PRIORITY INCIDENT: Medical School
  Type: Unauthorized SIS Access Attempt
  User: Unknown (brute force from 45.xxx.xxx.xxx)
  Target: Student Health Records
  Status: BLOCKED - Account lockout triggered

AUTOMATED RESPONSE:
  1. Source IP blocked at perimeter
  2. Security team notified
  3. Affected accounts flagged for review
```

AI Use Cases for Education

Use Case	Traditional	With AI
FERPA audit report	1-2 weeks	**30 min**
Student data breach investigation	Days	**Minutes**
Network troubleshooting	Hours	**Seconds**
Multi-campus security report	Manual	**Automated**
Research compliance evidence	Weeks	**Minutes**

Ransomware Protection

- **Early detection**: Behavioral anomaly alerts
- **Lateral movement**: Cross-system correlation
- **Automated response**: Isolation triggers
- **Recovery support**: Forensic evidence

Research Computing Support

Research IT prompt: "Analyze HPC cluster performance and security events for the genomics research group."

```
RESEARCH COMPUTING ANALYSIS
Cluster: HPC-GENOMICS | Nodes: 256 | Period: Last 7 Days
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
PERFORMANCE SUMMARY:
  Jobs Completed: 12,847
  Avg Queue Time: 2.4 hours
  Node Utilization: 87.3%
  Storage Used: 847 TB / 1 PB

SECURITY EVENTS:
  SSH Access: 2,341 sessions (all authorized)
  Data Transfers: 124 TB outbound
  Failed Auth: 23 (normal range)

COMPLIANCE STATUS:
  NIH Data Security: ✓ Compliant
  Export Controls: ✓ No violations
  IRB Data Handling: ✓ Audit trail complete

ANOMALY DETECTED:
  User: grad_student_47
  Activity: Unusual data export pattern
  Volume: 12 TB in 2 hours (10x normal)
  Status: Flagged for PI review
```

Grant Compliance Support

Framework	Coverage
NIH Data Security	Audit Trails
NSF Cybersecurity	Monitoring
ITAR/Export Control	Access Logs
HIPAA (Health Research)	PHI Tracking
CUI (DoD Research)	NIST 800-171

Network Visibility

- **Wireless**: 50,000+ concurrent devices
- **ResNet**: Dormitory network monitoring
- **Guest**: Visitor and event networks
- **IoT**: Smart building, lab equipment

AI-Powered Reporting & Remediation

Prompt: "Generate weekly review: security threats, infrastructure health, compliance audit, and cost optimization."

```
WEEKLY OPERATIONS REVIEW
Period: Last 7 Days | Events: 305,904 | Hosts: 34
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
SECURITY: 🔴 92 critical | 🟠 2,479 errors | ✅ 112K blocked

AUTOMATED ACTIONS:
  GeoIP enrichment: 112,412 events tagged
  SecOps tagging: 8,277 VPN events classified

COST OPTIMIZATION:
  Engineer time saved: ~13-22 hrs/week
  Storage savings: 80-90% (dedup+compression)

RECOMMENDATIONS:
  1. Review VPN SAML client configs
  2. Resolve syslog forwarding to backup
```

AI Report Capabilities

- **Weekly/daily reviews**: Automated summaries
- **Cost analysis**: ROI and savings metrics
- **Remediation playbooks**: Vendor CLI commands
- **Compliance evidence**: Audit-ready reports

Sample Prompts

- "Show FERPA-related access events"
- "Analyze ransomware indicators"
- "Generate incident report for ticket #1234"
- "What's causing the network slowdown?"

Deployment Options

On-Premises

- Campus data center
- Full data control
- Research compliance
- No cloud dependency

Cloud

- AWS, Azure, GCP
- Scalable architecture
- Customer-managed
- Full data control

Hybrid

- Campus collectors
- Central analytics
- Sensitive data local
- Flexible scaling

Why Education Institutions Choose LogZilla

Metric	Improvement
SIEM/storage costs	70-90% savings
Incident response time	85% faster
Compliance audit prep	90% faster
Multi-campus visibility	Unified

Education-Specific Benefits:

- **Budget-friendly**: Volume-based pricing
- **Student protection**: FERPA support
- **Research support**: Grant compliance
- **Scalable**: Grows with enrollment

Protect students, secure research, simplify compliance.

sales@logzilla.net | www.logzilla.net