

AI in IT Monitoring 2026 - Market Readiness and User Requirements for AI-Powered Monitoring Analytics

Based on market research practical project within the Business Informatics degree program at
OST University of Applied Sciences Eastern Switzerland

Executive Summary	2
Background.....	2
Key Findings.....	2
Research Base.....	2
The Evolution of Monitoring	3
The Market Gap.....	4
Current Market Landscape.....	4
Market Opportunity	4
Challenges Faced by Monitoring Teams.....	5
Defined scenarios	5
Most Valuable AI Use Cases	6
Scenario 1: Root Cause Analysis.....	6
Scenario 2: Migration Assistance	6
Scenario 3: Proactive Incident Management	6
Prioritization Result	6
What Customers Expect from AI	7
The study identified four essential requirements:.....	7
Across the board, the following requirements can be identified:.....	7
Trust as the Key Success Factor.....	8
Strategic Recommendations	8
E(i)xM design	9

Executive Summary

Background

Monitoring environments generate increasing amounts of operational data. However, identifying patterns, understanding root causes, and determining corrective actions often remain manual activities.

This report summarizes the results of a university-supported study investigating market readiness and user requirements for AI-powered monitoring analytics.

Key Findings

- Monitoring complexity is increasing.
- Root Cause Analysis is the highest-priority AI use case.
- Proactive Incident Management shows strong market potential.
- Trust is the primary adoption driver.
- Human oversight remains essential.

Research Base

- Monitoring professionals from organizations across Switzerland and the European Union
- PRTG and Zabbix environments
- Typical monitoring environments: 5,000–10,000 sensors / items
- Quantitative survey analysed by OST
- Qualitative expert interviews carried out by OST

The Evolution of Monitoring

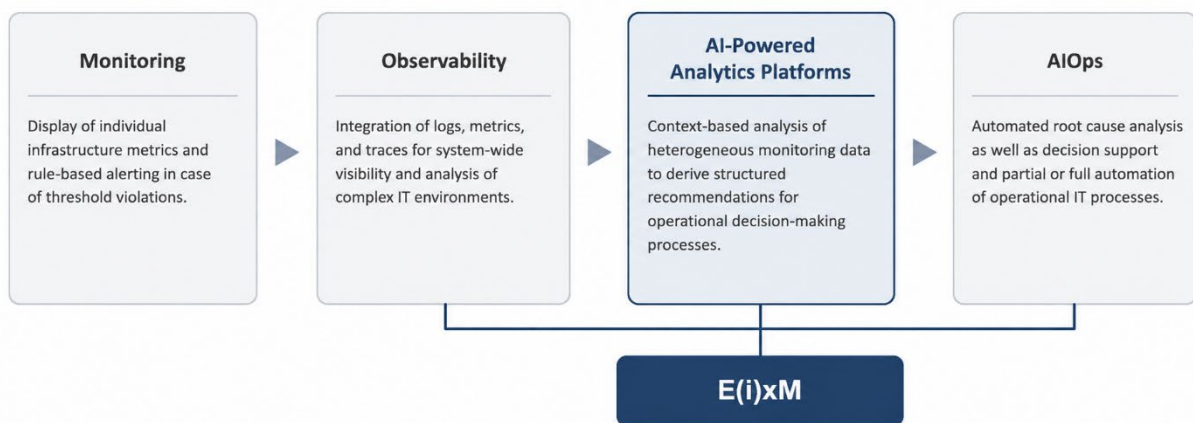
From Monitoring to AI-Powered Operations

Traditional monitoring solutions were designed to detect predefined thresholds and alert operators.

Modern environments require more:

- **Monitoring** Visibility into individual systems. Reliable monitoring. Limited analytical interpretation.
- **Observability** Correlation of metrics, logs, and traces. Cross-system visibility. Interpretation remains largely manual.
- **AI Analytics** Context-aware interpretation of monitoring data.
- **AIOps** Automation of operational decision-making. Advanced automation. Limitations: Complexity, cost, and implementation effort.

Organizations increasingly require intelligent support layers between traditional monitoring and enterprise-scale AIOps platforms.



The Market Gap

Current Market Landscape

Organizations today typically choose between:

- **Traditional Monitoring**
- **Observability Platforms**
- **Enterprise AIOps Platforms**

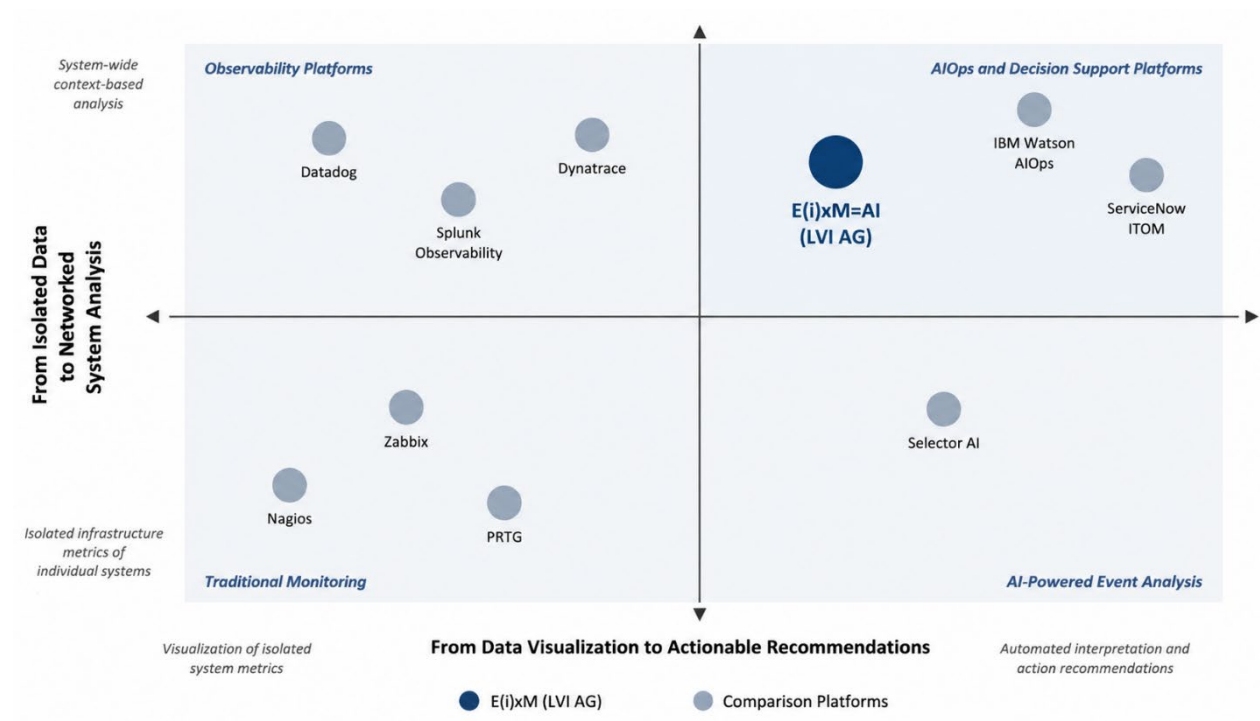
Market Opportunity

Many organizations require:

- AI-assisted analysis
- Operational recommendations
- Fast deployment
- Low implementation risk

without adopting full-scale enterprise AIOps.

E(i)xM AI's positioning matrix in the competitive landscape



Challenges Faced by Monitoring Teams

The study identified several recurring challenges:

- **Alert Fatigue** Teams struggle with excessive numbers of alerts.
- **Manual Root Cause Analysis** Investigations often require correlating multiple systems manually.
- **Resource Constraints** Monitoring teams frequently operate with limited staffing.
- **Growing Infrastructure Complexity** Cloud, hybrid, and distributed environments increase operational complexity.
- **Migration Effort** Monitoring platform transitions remain highly labor-intensive.

Defined scenarios

Scenario 1: Intelligent Root Cause Analysis

- **Problem:** Finding causes across interconnected systems is time-consuming.
- **AI Support:** AI correlates monitoring data and identifies likely causes.
- **Business Value:** Faster incident resolution and reduced operational effort.

Scenario 2: Automated Migration Assistance

- **Problem:** transition between different monitoring systems.
- **AI support:** AI analyzes existing monitoring structures and recommends an optimized migration path for the target platform.
- **Business Value:** it simplifies the migration of existing monitoring environments.

Scenario 3: Proactive Alarm Analysis (Closed-Loop)

- **Problem:** early detection of potential problems (predictive maintenance).
- **AI support:** AI continuously analyzes monitoring data, identifies anomalies, and recommends preventive actions before incidents become critical.
- **Business Value:** action recommendations are automatically generated and saved as structured tasks including Todos, assigned to a team.

Most Valuable AI Use Cases

Scenario 1: Root Cause Analysis

AI analyzes monitoring data and identifies likely causes of incidents.

Expected benefits:

- Faster diagnosis
- Reduced investigation effort
- Improved response times

Scenario 2: Migration Assistance

- Useful but project-based

Scenario 3: Proactive Incident Management

AI identifies anomalies before incidents become critical.

Expected benefits:

- Early intervention
- Reduced outages
- Better operational resilience

Prioritization Result

- Root Cause Analysis
- Proactive Incident Management
- Migration Assistance

What Customers Expect from AI

The study identified four essential requirements:

Transparency

- Users want understandable recommendations.
- Organizations are concerned about inaccurate or non-verifiable AI recommendations.

Control

- Final decisions should remain with humans.
- Autonomous interventions are rejected.
- Manual approval is a clear expectation.

Data Sovereignty

- Organizations require flexibility regarding data hosting and governance.
- On-premises or private cloud is preferred in many cases
- GDPR compliance is non-negotiable across the board.

Reliability

- Recommendations must be accurate, reproducible, and trustworthy.
- Growing awareness of cyber security risks
- Increasing demand for expert guidance during AI adoption

Across the board, the following requirements can be identified:

- Reducing the burden of repetitive alerts, particularly in relation to Scenarios 1 and 3
- Manual approval prior to AI intervention as a minimum requirement
- On-premises operation or private cloud hosting to ensure data sovereignty
- Traceable AI decisions, particularly for security-critical tasks
- Reduction of false alarms as a key performance requirement
- Cross-system process integration as an added value of LVI AG's add-on approach
- Vendor-neutral solutions to promote flexibility and customer loyalty

Trust as the Key Success Factor

Customers Want AI Assistance — Not AI Control

Across all interviewed organizations, trust-related requirements emerged as the most important adoption factor.

Preferred characteristics include:

- Human approval workflows
- Explainable recommendations
- Audit trails
- Controlled deployment models

The findings suggest that successful AI adoption depends more on trust than on advanced automation.

The study demonstrates that organizations are ready to adopt AI-supported monitoring solutions when transparency, control, and operational value are prioritized. Trust—not automation alone—will determine market success.

Strategic Recommendations

- Prioritize Root Cause Analysis and Proactive Incident Management.
- Build customer trust through transparency and human oversight.
- Introduce AI capabilities through focused pilot projects.
- Maintain data sovereignty through on-premises and private-cloud deployment options.

E(i)xM design

