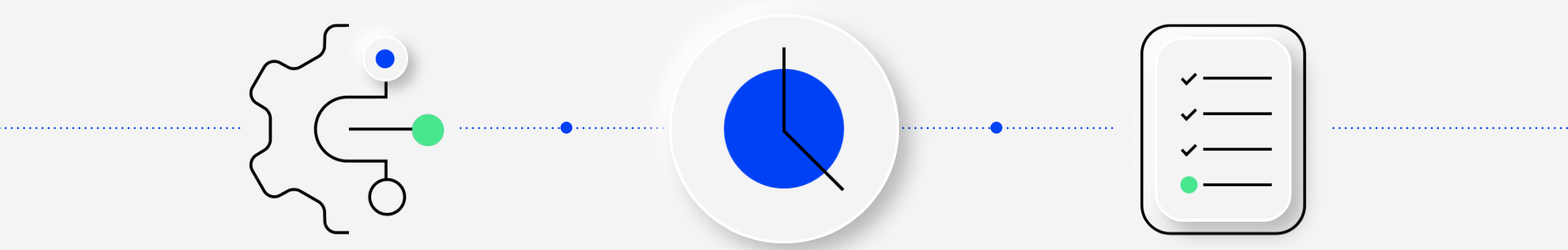
BigPanda

E-book

AIOps buyer's guide

Important considerations and criteria when evaluating an AIOps platform to reduce downtime.



Contents

Meeting customer expectations

Regardless of industry, it's imperative to avoid downtime, especially for customer-facing services. Customer expectations are higher than ever and increasingly more challenging to meet. They're looking for fast, always-on services. The IT teams with the agility to adapt their operations efficiently as customer demands evolve will excel.

With the rise of AIOps, more organizations are looking to address these demands with technologies such as automation and AI. According to a recent report from Enterprise Management Associates, 100% of IT leaders intend to increase the use of automation, AI, and AIOps in the next 6 to 18 months. AIOps enhances availability and efficiency by quickly processing massive volumes of data, enabling IT teams to catch and resolve more incidents faster.

Whether you're looking to optimize incident management or augment your current ITSM and observability tools, AI can help improve your current processes and outcomes. This guide outlines the importance of AIOps and identifies criteria to include in your requirements.

Challenges facing ITOps teams

Meeting high service availability and exceeding customer expectations is always on the to-do list for ITOps teams. Organizations face a rising number and variety of challenges, including:

- **Poor data utilization:** Organizations often use more than 20 observability and monitoring tools. Fragmented, noisy, and incomplete data complicates incident detection, correlation, and resolution.
- **Siloed workflows:** Silos prevent ITSM and ITOps teams from having full visibility of crucial business context in tickets. The result? Ticket backlogs, missed SLAs, excessive escalations, and missed critical issues.
- **Complex IT systems:** Mixed legacy and modern IT tools require substantial budgets and increase alert noise. Tool sprawl complicates maintenance, overwhelming teams and making it harder to identify critical incidents.
- **Uncertainty about AI:** Many organizations delay implementing AIOps due to misconceptions about high costs, slow ROI, the need for perfect data, and fears of job displacement.

Risks

When IT teams cannot address these challenges, they risk:

- Endless bridge calls to resolve communication breakdowns between teams due to workflow and data silos
- Slow response times due to inefficient, manual workflows requiring operators to search for relevant information to understand incidents
- Increased IT team stress due to data overload and lack of visibility into the relationships between alerts
- Unhappy stakeholders and customers resulting from missed SLAs due to the inability to identify root causes quickly, compounded by a high ticket volume

Benefits of better context

AIOps uses various technologies, including generative AI and open-box machine learning. These platforms ingest multiple data sources, normalize different types of IT infrastructure data, and provide clear context so teams can quickly detect issues, identify the root cause, and resolve incidents.

Context is crucial. Context provides IT teams the information they need to find, understand, and resolve incidents faster, more consistently, and at scale. As a result, they can:

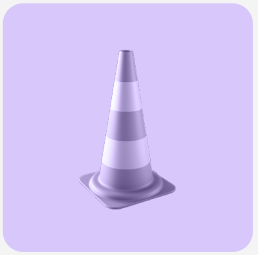
- Improve incident analysis by providing operators with the necessary information to resolve incidents on the first try.
- Generate clear, centralized IT ecosystem visibility, including actionable insights to improve and optimize resolution processes.
- Correlate alert data from disparate sources and provide a single source of information free of any noise.
- Enhance incident remediation with automation capabilities such as runbook automation, collaboration notifications, and automatic ticketing in ITSM tools without contextual blind spots.

By offering comprehensive insights, AIOps ensures that teams can make informed decisions promptly. AIOps unifies ITOps and ITSM teams by simplifying the hand-off of information and supporting collaboration to speed up incident-response workflows.

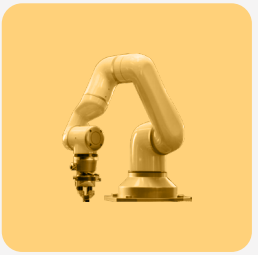
Full IT infrastructure visibility

Reduced alert noise

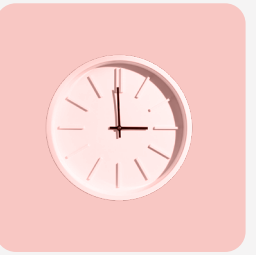
Faster incident management



Automated workflows



Improved service uptime



"69% of respondents indicated that at least 25% of the mean time to resolution is wasted."

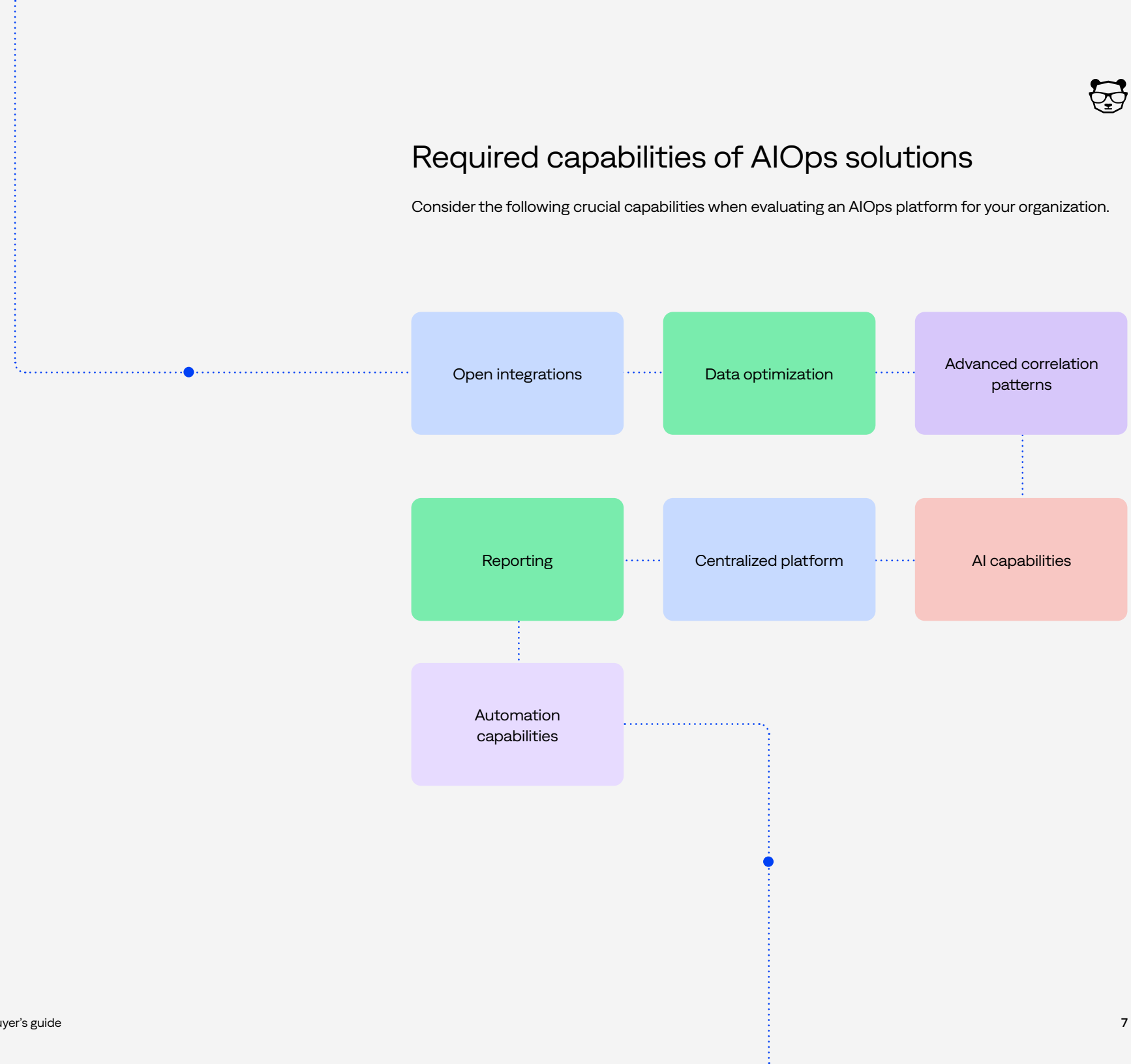
"Real-world incident response, management, and prevention," EMA Research, January 2024

Desired solution outcomes

Reduce time to value	Unlike legacy tools, AIOps solutions offer quick implementation and value, setting a solid foundation for scaling across IT infrastructure.
Improve the value of ITSM outcomes	AIOps enriches and augments data to facilitate smoother handoffs between ITSM and ITOps teams for quicker remediation.
Increase operational efficiency	AIOps platforms should automate tedious tasks and accelerate incident management, helping IT teams focus on innovation.
Elevate your infrastructure	AIOps should enhance existing tools and provide quick insights and improvements, regardless of your data's initial quality.

Required capabilities of AIOps solutions

Consider the following crucial capabilities when evaluating an AIOps platform for your organization.



Open integrations

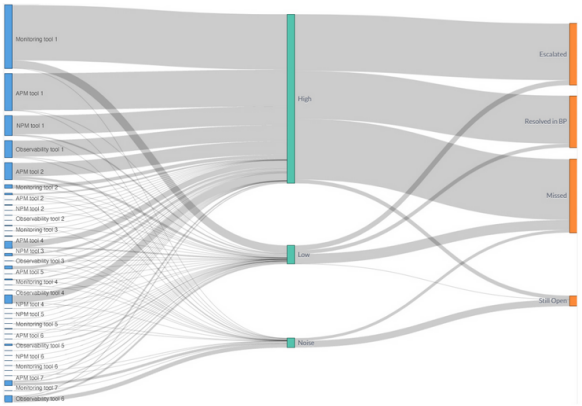
On average, IT organizations manage 20 or more monitoring and observability tools. Each tool is responsible for a specific application, infrastructure, or service. Managing these tools individually is difficult due to all the alerts and noise they create.

Strong AIOps platforms can integrate any data source into their AIOps solution. For example, they support:

- **Standard prebuilt integrations:** Ready-to-go integrations for the most popular observability and monitoring tools (This is a must-have.)
- **Custom integrations:** Easy setup through an API call or an easy-to-use UI interface
- **Open and agnostic:** Ingestion of all types of data from CMDB, change, runbooks, service maps, metrics, logs, and traces

Data optimization

An AIOps solution should process data automatically without human intervention to provide cohesive, clean visibility into an IT ecosystem. Platforms can do this through data aggregation, deduplication, normalization, and enrichment. AIOps administrators should be able to manage how the platform manipulates information to fit their organization's specific use case and business needs.



Sankey diagram showing the monitoring tools that send the most alerts.

Advanced correlation patterns

Comprehensive correlation provides IT teams with contextual, accurate insights, enabling faster incident detection, prioritization, assignment, and remediation. An AIOps platform should easily set up and fine-tune correlations as you add new sources. Approaches and techniques include those based on:

- **Time:** Uses the most basic correlation approach
- **Rules or tags:** Bases variables on specific values or tags
- **History:** Learns from previous events and uses past data for new events

AI capabilities

AIOps can significantly enhance ITOps efficiency and effectiveness, providing tools for high availability and quick incident resolution. As AI technology becomes more prevalent, it must have the following features:

- **Accurate AI:** Choose an AIOps platform that uses comprehensive datasets from diverse sources — including MELT, ITSM, and CMDB — to produce accurate, insightful outputs.
- **AI transparency:** Ensure the AI is open-box and fully transparent, allowing operators to understand the processes behind event grouping and alert correlation.
- **Comprehensive data analysis:** The platform should integrate and enrich data from various sources, providing operators with a complete, actionable picture of incidents.
- **Contextual outputs:** The AI should deliver clear, actionable insights and integrate directly with tools like ITSM to provide relevant information where users work most.

EMA survey respondents identify important factors to unify service and operations:

56%
Cross-functional processes and workflows

53%
Shared and accessible data

Centralized platform

Unifying data, correlating alerts, and providing AI-augmented context for faster remediation gives operators a complete understanding of incidents. Consolidating these actions into a single, accessible view ensures operators have all the necessary information at their fingertips. Additionally, the platform should organize alerts by specific domains and allow operators to manage, assign, investigate, and escalate incidents to facilitate quick resolution.

Reporting

Reporting and dashboards are crucial to help IT leaders assess alert quality, identify the need for tool rationalization, and highlight gaps. Essential reporting capabilities include:

- **Out-of-the-box:** Ready-to-use dashboards and visualizations for comprehensive insights into the IT ecosystem
- **Actionable insight:** Dynamic metrics to help IT teams rationalize the technology stack, identify process gaps, and demonstrate organizational value
- **Flexible, transparent:** Direct access to underlying data tables for further analysis

49%

of EMA respondents cite workflow automation as critical to unifying services and operations.

Automation capabilities

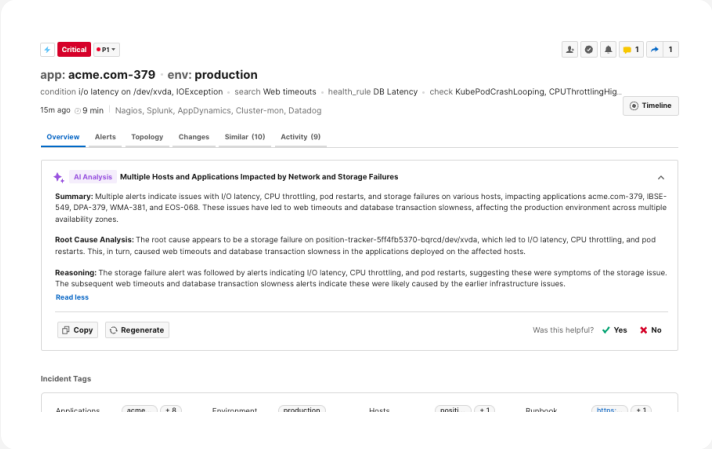
The promise of AIOps centers around simplifying the roles of operators. IT teams are overwhelmed by endless information searches, long bridge calls, and alert noise. As a result, look for platforms that can help automate tedious tasks to free up time. Automation capabilities should include:

- **Ticketing:** Integration with ITSM tools to automatically generate and update tickets with additional context for easier collaboration and remediation
- **Notifications:** Automation of notifications to the appropriate remediation teams to ensure seamless collaboration
- **Runbooks:** Integration with third-party automation tools to execute runbooks during incidents to prevent outages and ensure SLAs

NYSE

"[The AIOps tool] saves us a lot of time and lets us focus on resolving problems instead of combing through thousands of alerts to find out what the problems are."

Chuck Adkins
CIO, New York Stock Exchange



Next steps

Learn more about the BigPanda platform.

Explore case studies to learn how organizations across industries benefit from AIOps.

Learn more in our practical guide to AIOps implementation.

Why BigPanda

The BigPanda AIOps platform provides IT teams with the context they need to quickly remediate incidents, freeing operators' time to work on more innovative projects. BigPanda AIOps unifies data, tools, and processes across observability, operations, and ITSM teams, providing incident data up front, quickly, and consistently. With full incident context, you can remediate incidents at scale, improve operator efficiency, and increase application and service availability.

Reduce downtime

Proactively identify potential outages with automated GenAI analysis. Automate root cause analysis to expedite resolution and support uninterrupted user experiences.

Speed incident resolution

Standardize fragmented data, workflows, and processes with BigPanda open and agnostic unified data fabric. Identify relationships and generate an actionable alert stream with our open-box AI.

Maximize IT investments

Use Unified Analytics dashboards to gain end-to-end visibility of your IT environment. Identify opportunities for strategic improvements and consolidation to improve efficiency and reduce costs.

Scale incident management

Enhance operations by automating manual tasks such as notifying teams via Slack, Microsoft Teams, and Asana. Transform incidents into actionable tickets with custom rules and integrations into ITSM tools like ServiceNow.

bigpanda.io