Market Guide for AIOps Platforms

Published 30 May 2022 - ID G00750431 - 21 min read

By Analyst(s): Pankaj Prasad, Padraig Byrne, Gregg Siegfried

Initiatives: Infrastructure, Operations and Cloud Management

> AIOps platforms enable decision making across design, deploy, execute and operate activities by automated contextualization of large, varied volumes of operational data. I&O leaders should use AIOps platforms to analyze and share application life cycle insights, making digital business observable.

Overview

Key Findings

■ One of the main barriers to implementing artificial intelligence for IT operations (AIOps) platforms is the difficulty measuring their value and a lack of understanding of benefits derived.

■ Although I&O leaders continue to take a cautious approach that is dominated by small incremental goals and practical outcomes rather than an all-inclusive approach, AIOps platform adoption is growing rapidly across enterprises.

■ Data management costs and complexity are becoming a concern for many enterprises that have adopted AIOps platforms as they expand their use. The hurdles include optimizing data storage, controlling cost, improving data quality at the source and, of late, data transmission.

■ Enterprises are replacing some traditional monitoring tool categories by embedding them within AIOps platforms. For example, virtual network monitoring, observability and infrastructure as a service (IaaS) monitoring are being done entirely within AIOps platforms, especially if the enterprise has its entire IT footprint in the cloud.

■ Enterprises continue to increase their use of AIOps platforms across various aspects of IT operations management (ITOM) and mature their use cases across DevOps and site reliability engineering (SRE) practices.

Recommendations

I&O leaders responsible for infrastructure, operations and cloud management should:

- Focus on tangible and incremental business outcomes with quantitative value-based proof points. Avoid the AIOps hype.

- Leverage AIOps platforms for scenarios like adaptive anomaly detection or system-centric anomaly detection. Entity-centric anomaly detection is better served by monitoring tools.

- Target productivity outcomes when using AIOps platforms; for example, leverage them to enhance workflows and to improve efficiency of IT personnel.

- Create an operations model to provide metadata and insights as a service to different departments such as finance, sales and marketing.

Market Definition

AIOps platforms analyze telemetry and events, and identify meaningful patterns that provide insights to support proactive responses. AIOps platforms have five characteristics:

1. Cross-domain data ingestion and analytics

2. Topology assembly from implicit and explicit sources of asset relationship and dependency

3. Correlation between related or redundant events associated with an incident

4. Pattern recognition to detect incidents, their leading indicators or probable root cause

5. Association of probable remediation

Market Description

AIOps platforms enhance a broad range of IT practices, including I&O, DevOps, SRE, security and service management. The central functions of AIOps platforms are discussed below.

Cross-Domain Data Ingestion and Analytics

An AIOps platform can ingest, index and normalize events or telemetry from multiple domains, tools or sources, including infrastructure, networks, applications, the cloud or existing monitoring tools (for cross-domain analysis) (see Note 2). The platform must further enable data analytics using machine learning (ML) at at least two points, including:

- Real-time analysis at the point of ingestion (streaming analytics)

- Historical analysis of stored data

Topology Discovery

AIOps platforms periodically discover and assemble unified topologies of IT assets, including applications, across domains. Topologies can include physical proximity, logical dependence or another dimension that captures the relationship between IT assets and services.

Event and Telemetry Correlation

The AIOps platform automatically correlates and compresses events across telemetry domains or sources, reducing unnecessary human intervention. The correlation combines time and topology to group-related events.

Pattern Recognition and Clustering

An AIOps platform processes event and telemetry data to detect or predict important events or incidents. The platform uses historic data for an initial baseline and continually learns and refines individual patterns of important events based on historical data, real-time streaming data, from operator input and reinforcement mechanisms.
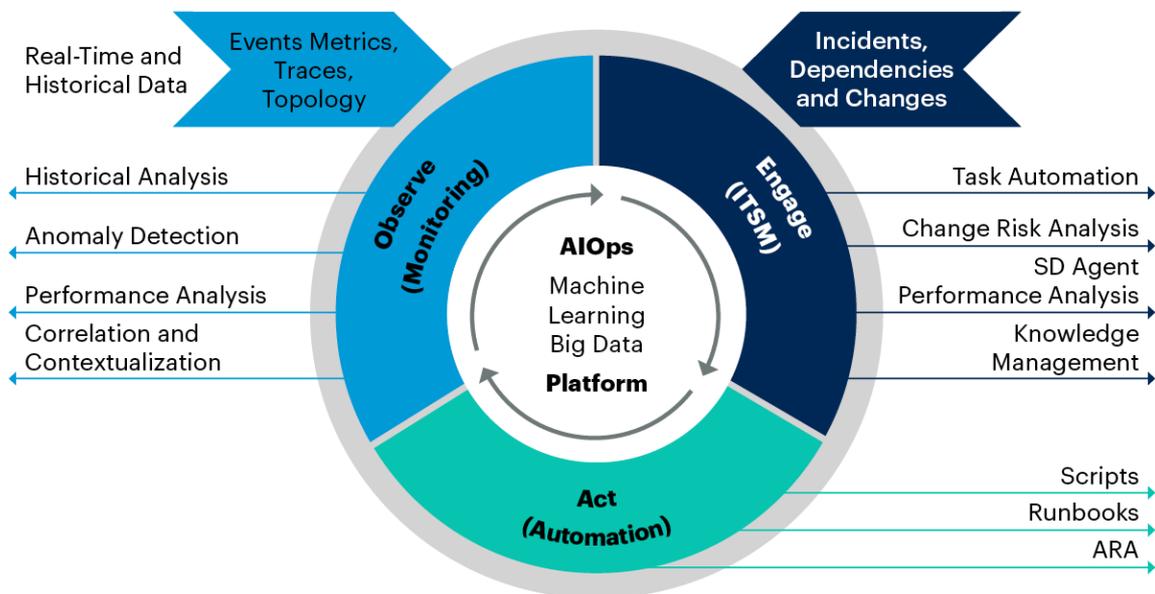
Remediation

The AIOps platform continuously learns and improves associations between each important event and the operations response by either explicit operator specification or observation. The AIOps platform might offer a recommendation, automate a response or trigger an external automation system.

The goal of AIOps platforms is to curate and enhance the quality of ingested data so I&O leaders can drive multiple use cases relevant to the appropriate practice or persona. For example, pattern discovery can help forecast emerging behavior, relationships across IT entities, and benchmarking behavior (of IT artifacts, users and agents) to identify anomalies and provide relevant context to business owners. Analytics also facilitates automated insights, eases root cause determination and enables automated actions for resolving identified issues (see Figure 1).

Figure 1: AIOps Platform Enabling Continuous Insights Across IT Operations Monitoring (ITOM)

AIOps Platform Enabling Continuous Insights Across IT Operations Monitoring (ITOM)

Real-Time and Historical Data

Events Metrics, Traces, Topology

Incidents, Dependencies and Changes

Observe (Monitoring)

Engage (ITSM)

Act (Automation)

AIOps Machine Learning Big Data **Platform**

Historical Analysis

Anomaly Detection

Performance Analysis

Correlation and Contextualization

Task Automation

Change Risk Analysis

SD Agent Performance Analysis

Knowledge Management

Scripts

Runbooks

ARA

Source: Gartner
735577_C

Gartner

Market Direction

AIOps: Analytics Versus AIOps Features Versus AIOps Platforms

Many vendors in the ITOM space claim to deliver AIOps capabilities, several claim they deliver an AIOps platform, and some even claim to be the embodiment of AIOps. Gartner views AIOps platforms to be a market defined by a combination of needs and reasonably similar vendor responses to those needs in the form of products. AIOps by itself is not a market. A product may provide one or more functions of an AIOps platform or it may have certain analytics or AI capabilities.

To that extent, Gartner has come across three distinct market categories:

- **Data and analytics tools** are products that enable the building of solutions that may reflect the architecture of an AIOps platform but are capable of one-off or limited use cases to address a specific challenge.

- **AIOps features** are categorized as IT tools that apply AI component technologies to their domain of monitoring or management.

- **AIOps platforms** deliver all of the five defining functions listed above.

Continued Interest and Growth

AIOps continues its growth and influence on the overall ITOM market, with a projected market size of about $2.1 billion in 2025 at a compound annual growth rate (CAGR) of around 19% (see Market Opportunity Map: IT Operations Management, Worldwide). Adoption and direction are being heavily influenced by three separate but ultimately related areas:

- Digital business transformation

- Transitioning from a reactive posture to a proactive approach

- The need to make digital business observable

Digital Business Transformation

Digital business transformation is driving the AIOps market due to the resulting proliferation of new applications and services that generate more and more data of varying types, making their analysis ever more critical and difficult. With data volumes reaching or exceeding gigabytes per minute across a dozen or more different domains, it is no longer possible, much less practical, for a human to analyze the data manually in service of operational expectations.

Transitioning From a Reactive Posture to a Proactive Approach

As organizations continue to undertake digital transformation, IT operations no longer has the luxury of responding to issues after they occur. Instead, it must become proactive, get more involved in the entire value stream and, at a minimum, work to address potential issues before they impact user experience.

The Need to Make Digital Business Observable

Observability is inclusive of information correlated based on data across the full stack including infrastructure, applications, digital experience, business key performance indicators (KPIs) and social sentiment. Observability also includes active interrogation of systems for information required situationally, yet not already available via monitoring. AIOps platforms help in the discovery of patterns, relationships and dependencies among these elements, making digital business observable for the relevant personas.

Do-It-Yourself Architectural Approach

Enterprises that have achieved a level of maturity using AIOps platforms tend to focus more on the outcomes rather than the platform. Gartner has come across scenarios where organizations are taking a do it yourself (DIY)-architectural approach using one or more of the following strategies and tools:

- **Data lake:** This involves setting up a two-tier architecture where data storage is relegated to a low-cost tier as compared to the premium, high-cost tier where the organization has its existing models, algorithms and dashboards. Data is stored in the low-cost tier and streamed into the premium tier for analysis.

- **Transport layer:** This includes using an independent data transport layer to stream data from one or multiple sources to multiple destinations. In this scenario, organizations seek better control over data transport, including data compression and the ability to send large volumes and/or selective data to multiple destinations.

- **Data capture and data pipelines:** Some organizations prefer building their own data capture capability, for example, by using Apache Kafka. Compared to the first two scenarios, this approach is rare, but interest in it is growing.

- **Analytics:** The ability to automate analytics or apply machine learning in a DIY scenario is still a challenge. Organizations usually rely on basic analytics, such as trend analysis and anomaly detection, or rely on visual analytics where relevant information is displayed on screen and the IT operator visually inspects the data displayed for insights. Very few organizations leverage ML in a DIY scenario, and, when they do, the use cases are limited.

- **Visualization:** Displaying data and insights in easy and meaningful ways is usually done through tools like Grafana or Kibana.

Market Analysis

AIOps platforms have existed for a number of years, yet successful deployments require time and effort. The time to value of many AIOps platform tool deployments is measured in months or years, which has led to dissatisfaction and disillusionment with the market segment.

> **Yet, there is no doubt: There is no future of IT operations that does not include AIOps.**

This is due to the rapid growth in data volumes and pace of change (exemplified by rate of application delivery and event-driven business models) that cannot wait on humans to derive insights. It is simply impossible for humans to make sense of thousands of events per second being generated by their IT systems.

To get a clearer picture of how the market is evolving and where vendors are positioned relative to one another, consider the following AIOps attributes:

- Explainability and interpretability

- Data ingestion and handling

- Machine learning analytics

- Automated insights

- Adaptive remediation

Explainability and Interpretability

There are concerns around the use of AI within IT operations. Many IT operations staff have experience with misbehaving automation tools that have misfired, run amok or otherwise wreaked havoc. To earn trust, IT operations teams must be transparent about their use of AI, how models are created and how they should be used.

AIOps vendors are starting to include explainable AI and interpretable AI in their platforms and tools. Explainable AI systems allow for the understanding of how models are created; interpretable AI systems facilitate the understanding of the output of AI systems. Not all AIOps systems will be explainable, but all will be able to be interpreted.

AIOps platforms and tools currently have little explainability inside them, functioning primarily as a black box. Some basic elements that are being implemented include the use of probabilities, rather than binary output, for outcomes. Others include the ability to see the root cause path that was used to come to a certain conclusion. However, the majority of the calculations and analysis that these tools perform will remain hidden to the user.

If AIOps is to gain widespread traction and trust, more must be done to improve both explainability and interpretability of AIOps functions. See Innovation Insight for Bias Detection/Mitigation, Explainable AI and Interpretable AI for more details on these topics.

Data Ingestion and Handling

AIOps platforms must be able to analyze data at rest (historical) and data in motion (real-time streaming). These platforms allow for the ingestion, indexing and storage of logs, event data, metrics, traces, and graph and document data (see Note 2).

These tools for IT operations must analyze data directly at the point of ingestion, in real time, without requiring data to be saved to a database before it can be analyzed. They also must provide a correlated analysis across multiple streams of real-time and historical data.

Machine Learning Analytics

AIOps platforms use the following types of analytics approaches:

- **Statistical, probabilistic analysis.** A combination of univariate and multivariate analysis, including the use of correlation, clustering, classifying and extrapolation on metrics captured across IT entities.

- **Automated pattern discovery and prediction.** Discovering patterns, clusters or groups of correlations in historical and/or streaming data. These patterns may then be used to predict anomalies with varying degrees of probability.

- **Anomaly detection.** Using the patterns discovered by the previous components to determine normal behavior and then to discern departures from that normal behavior, both univariate and multivariate. Transcending the mere detection of outliers, they must be correlated with business impact and other concurrent processes such as change management to be fully useful and not just create more alert noise.

- **Probable cause determination.** Pruning down the network of correlations established by the automated pattern discovery and ingestion of data to define causality chains linking cause and effect.

- **Topological analysis.** Using application, network, infrastructure or other topologies to provide contextualized analysis. Deriving patterns from data within a topology will establish relevancy and illustrate hidden dependencies. Using topology as part of causality determination can greatly increase its accuracy and effectiveness.

- **Adaptive prescriptive advice.** Suggesting solutions to resolve an issue. These suggestions may be based on a database of historical solutions (institutional knowledge) to recurring problems or determined via crowdsourcing. Over time, the tool should identify the most relevant solution from multiple possibilities that may exist.

Automated Insights

Reduce the visual overload for IT operators by identifying interesting data instead of treating the display screen as a dumping ground. IT operators should not have to observe two or more graphs simultaneously and perform visual analytics; rather, the platform should analyze signals, identify areas that need human attention, and communicate them using the most effective means possible including but not limited to visual interfaces, notifications via collaboration tools, or other interfaces.

Adaptive Remediation

As the technology matures, users will be able to leverage prescriptive advice from the platform, enabling the action stage. The steps for this are shown in Figure 2.

The Future of AI-Assisted Automation: Triage and Remediation of Problems
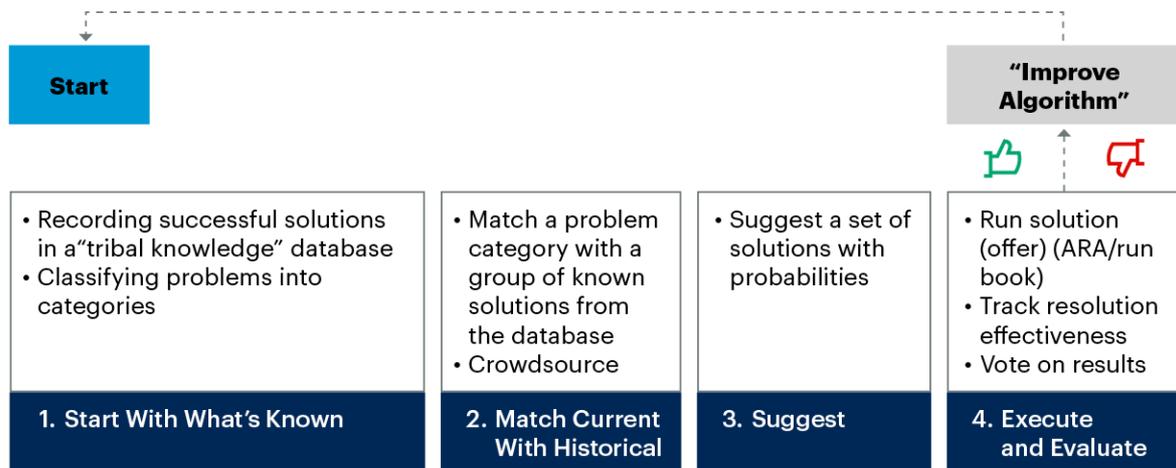
Source: Gartner

735577_C

Gartner

The true value of an AIOps platform is in its ability to identify the most appropriate action from multiple possible solutions for the situation at hand. Choosing a prescriptive solution from an available repository can be done through run book automation and does not need specialized AI technologies. The likely candidates for such nonadaptive automation are those that are low-risk and can cause relatively little damage if they fail or result in unexpected side effects.

Precedence of Use Cases Over Nomenclature

I&O leaders have stopped assuming AIOps as a terminology is self-explanatory. Over the past 12 months, we observed many Gartner clients discussing their requirements in the form of use cases rather than using AIOps terminology. If the use cases were better served by existing monitoring technologies, AIOps platforms were not shortlisted. If the use cases envisioned by enterprises were advanced compared to existing monitoring capabilities, a DIY approach was applied.

AIOps platforms were usually shortlisted for one or more of the following use cases:

- Complex anomaly detection

- Event management and correlation

- Enhanced diagnostic and root cause analysis

- Centralized log analysis

- Behavior analysis (across customer journeys or for system behavior)

- Centralized dashboarding

- Predictive capability

- Impact analysis (as it relates to user and business)

- Incident remediation

Efficiency Over Effort

Mature organizations prefer to measure outcomes and ROI in terms of efficiency gains. For example, executives in many organizations are not keen on focusing on how many incidents were reduced, whether as a result of AIOps or other reasons. Their interest is in benefits that are tangible to the business, like enhanced efficiency and improved productivity.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

AIOps platform vendors have a broad range of capabilities that continues to grow. Vendors differ in their data ingest and out-of-the-box use cases made available with minimal configuration. In Table 1, we provide a representative sample list of vendors providing AIOps platform functionality (see Note 1).

Table 1: Representative Vendors in the AIOps Platforms Market

(Enlarged table in Appendix)

Vendor	Product, Service or Solution Name
BigPanda	BigPanda
BMC	TrueSight Operations Management, Helix Platform
Broadcom (CA Technologies)	DX Operational Intelligence
Devo	Devo
Digitate	ignio
Elastic	Elasticsearch
GAVS	Zero Incident Framework (ZIF)
IBM	IBM Cloud Pak for Watson AIOps
Interlink Software	Interlink Software
Logz.io	Log Management
Moogsoft	Moogsoft
OpsRamp	OpsRamp Platform
PagerDuty	PagerDuty
ScienceLogic	ScienceLogic SL1
ServiceNow	IT Operations Management (ITOM)
Splunk	Splunk Enterprise, Splunk Cloud Platform
StackState	StackState
Sumo Logic	Sumo Logic
Vitria	VIA AIOps
VuNet	vuBJM
Zenoss	Zenoss

Source: Gartner (May 2022)

Market Recommendations

Use a Top-Down AIOps Framework

AIOps lends itself to use cases spanning the hierarchy from the IT operator up to a line of business (LOB) owner or even a CIO. It can, for example, enable a service-level view, provide behavior analysis (related to both systems and users) and provide visibility into business impact.

In practice, these platforms only provide event correlation capabilities as an out-of-the-box use case, making them initially relevant for IT operators. Platform users are tasked with creating outcomes relevant to other roles, such as I&O leaders, system administrators, architects and LOB owners.

Gartner recommends starting by creating a roadmap with an end-goal objective to be achieved through the use of AIOps platforms. For example, within a monitoring strategy, determine how AIOps can transform data for relevance to the target persona and how it helps address the purpose for the respective persona. Follow this by mapping out the steps leading up to the objective, starting with the current state of visibility within IT operations (e.g., noisy events, static-threshold-based alerts or leveraging dynamic thresholds) For more information, see Solution Path for Adopting AIOps.

Select the AIOps platform best-suited to deliver out-of-the-box capabilities for the first step on the roadmap. The selected vendor should have capabilities or a roadmap aligned to the organization's roadmap (for example, helping the organization to advance from event correlation to dynamic thresholds to behavior analysis with minimal effort). Watch for portability challenges in these platforms as use cases mature (see Note 3).

When building a business case for AIOps' return on investment, I&O leaders must discuss with vendors the expected time to value of their implementation. In many cases, a limited proof of concept would be expected to demonstrate how integrations would work in a realistic setting.

Automation for Insights

Some enterprises have a goal leading up to automated remediation of identified anomalies. Any automation initiative is based on a certain level of standardization. This is a major inhibitor of large-scale deployment of automated actions. IT organizations with a high level of maturity prefer automated insights over automated actions as a tangible goal.

Relevance for Diverse Personas

AIOps platforms are adopted by different teams, like DevOps, SRE, IT operations, cybersecurity (see Magic Quadrant for Security Information and Event Management) and business leaders. The use cases and raw data required differ based on the team adopting the platform and its maturity.

DevOps

Log analytics was a primary requirement for DevOps teams a couple of years ago, which has now expanded to include metrics and traces as primary requirements. As the DevOps practice matures, AIOps use cases broaden from a focus on preproduction to include production metrics like user engagement, quality and business relevance. This creates a need for new KPIs, comparison across multiple versions, and a product and platform focus. Considering this scenario, select platforms that can ingest instrumented data (traces, metrics and logs) and ease the effort to provide platform and product views for DevOps.

IT Operations

Metric and log ingestion, followed by analytics are the primary requirements for I&O teams. The journey starts with event correlation and, as the team matures, broadens to analysis of metrics and logs followed by behavior analytics of systems and users. The primary goal here is anomaly detection, diagnostic information and root cause analysis. Other use cases include automation, for example, automated actions through integrations or through scripts, or automated workflows. Select platforms that offer the flexibility to ingest events, logs and metrics, and offer out-of-the-box capabilities for at least one prioritized use case for I&O.

Business

User engagement, efficiency, productivity and behavior analysis to help drive better decisions are the key requirements for business leaders. AIOps insights are progressively expanded, starting with correlation of user impact based on IT and broadened to include qualitative KPIs like the efficiency and productivity of technology, people and existing processes. In mature organizations, staff reduction is not the driving force behind automation. For such scenarios, select platforms that focus on clustering and demographics, and provide causal insights across diverse datasets, including sentiment and satisfaction.

SRE

The goals of SRE are similar to IT operations and DevOps use cases. Typically, these are mature use cases across both practices. For example, event correlation and log analytics are not the primary objective of SRE teams, but the analysis based on outcomes of event correlation and log analytics are important inputs toward improving resilience. Their focus area includes IT architecture assessments. For SRE use cases, select platforms that provide real-time topological and dependency insights for the IT architecture as one of the primary use cases and offer ease of comparative temporal and spatial analysis for multiple scenarios.

Acronym Key and Glossary Terms

APM	Application performance monitoring
BAM	Business activity monitoring
DA	Domain agnostic
DC	Domain centric
ITIM	IT infrastructure monitoring
ITOM	IT operations management
ITSM	IT service monitoring
NLP	Natural language processing
NPMD	Network performance monitoring and diagnostics
SIEM	Security information and event management

Evidence

[1] **Gartner's 2020 Achieve Business Agility With Automation, Continuous Quality and DevOps Study** was conducted online from June through August 2020 among 205 respondents working for service providers, cloud providers, and end-user organizations in North America and Western Europe that have deployed or are using DevOps. Qualified organizations had at least $500 million in annual revenue and were required to primarily operate in the banking and financial services, government, insurance, healthcare, and retail industries.

Respondents were required to work in their organization's IT function, have a job title less senior than C-suite level and be two or more layers away from the most senior executive in their organization. Respondent's role had to be primarily focused on application development, infrastructure and operations, or business intelligence and information management. In these focus areas, they were also required to perform relevant roles/activities. The study was developed collaboratively by Gartner analysts who follow digital business trends and Gartner's Research Data and Analytics team.

Results of this study do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

Over the past 12 months, AIOps formed part of the conversation in 40% of all inquiries with Gartner clients on IT performance analysis. The topics of these inquiries included:

- Technology and market awareness.

- Platform selection.

- Build versus buy decisions.

- Optimization of existing AIOps deployments.

- Deployment strategy in case of new deployments.

- Pros and cons of a common platform shared across DevOps, I&O, security and SRE teams.

- Multiple AIOps use cases within and outside IT to aid visualization, decisions and diagnostics.

- The pandemic saw a majority of use cases related to event correlation.

Note 1: Representative Vendor Selection

The vendors listed in this research were picked as a sample based on having one or two of the following characteristics:

- Domain-agnostic solutions with the ability to ingest data from multiple sources, including historical and real-time streaming.

- Different offerings that include proprietary, open-source, free and commercialized versions, including deployment that cuts across on-premises and SaaS-based options.

- Products used or discussed by Gartner clients in interactions with analysts.

Vendors categorized under the APM market do have significant AI capabilities but are not included as they rarely come up outside of the APM use case.

Note 2: Data Sources for AIOps Platforms

Data sources for AIOps platforms include:

- API

- Application logs

- CRM data

- Customer data

- Events

- Graph

- ITSM

- Metadata

- Metrics

- Social

- Traces

- Wire

Unfortunately, no matter how large or how frequently updated a given dataset is, restriction to a single data source tends to limit the insights into system behavior. Modern IT systems — with their modularity and dynamism — require a multiperspective approach to understand what is happening as they are being observed.

Note 3: Portability

As an enterprise's AIOps adoption matures with functional models and quality outcomes, vendor switching becomes difficult. Switching to a different vendor to replicate existing high-quality dashboards will take time, which eliminates any value gained through direct cost savings. Gartner has observed a reluctance to switch vendors during contract renewal precisely for this reason in enterprises with more mature deployments.

The need for viable options to challenge incumbents has given rise to questions regarding portability of algorithms across vendors. This need comes from a few mature enterprises, where AIOps adoption has matured within the enterprise. The market is still at a high-growth stage, and it will be at least a couple of years before we see rising pressures from enterprises for portability and a response from vendors as a differentiator.

Some vendors are coming up with transfer learning, which is still in nascent stages. In its simpler form, end users are offered the option of training a selected model by using historical data. The results from the algorithm are compared against real-time results. Once the outcomes show a fair amount of accuracy with acceptable error margins, the end user can use the same algorithm for analyzing real-time data. This capability works best between preproduction and production environments or between the edge and the data center environments. Evolution of more complex use cases will require maturity and advanced skills on both the vendor and end-user side.

Document Revision History

Market Guide for AIOps Platforms - 6 April 2021

Market Guide for AIOps Platforms - 7 November 2019

Market Guide for AIOps Platforms - 12 November 2018

Market Guide for AIOps Platforms - 3 August 2017

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Infographic: AIOps Architecture for Analyzing Operational Telemetry

Use AIOps for a Data-Driven Approach to Improve Insights From IT Operations Monitoring Tools

Monitoring and Observability for Modern Infrastructure and Applications

2022 Planning Guide for IT Operations and Cloud Management

Assess Approaches to AIOps for a Comprehensive Solution

Market Share Analysis: ITOM, Performance Analysis Software, Worldwide, 2020

Table 1: Representative Vendors in the AIOps Platforms Market

Vendor	Product, Service or Solution Name
BigPanda	BigPanda
BMC	TrueSight Operations Management, Helix Platform
Broadcom (CA Technologies)	DX Operational Intelligence
Devo	Devo
Digitate	ignio
Elastic	Elasticsearch
GAVS	Zero Incident Framework (ZIF)
IBM	IBM Cloud Pak for Watson AIOps
Interlink Software	Interlink Software
Logz.io	Log Management
Moogsoft	Moogsoft
OpsRamp	OpsRamp Platform
PagerDuty	PagerDuty
ScienceLogic	ScienceLogic SL1
ServiceNow	IT Operations Management (ITOM)

Splunk	Splunk Enterprise, Splunk Cloud Platform
StackState	StackState
Sumo Logic	Sumo Logic
Vitria	VIA AIOps
VuNet	vuBJM
Zenoss	Zenoss

Source: Gartner (May 2022)