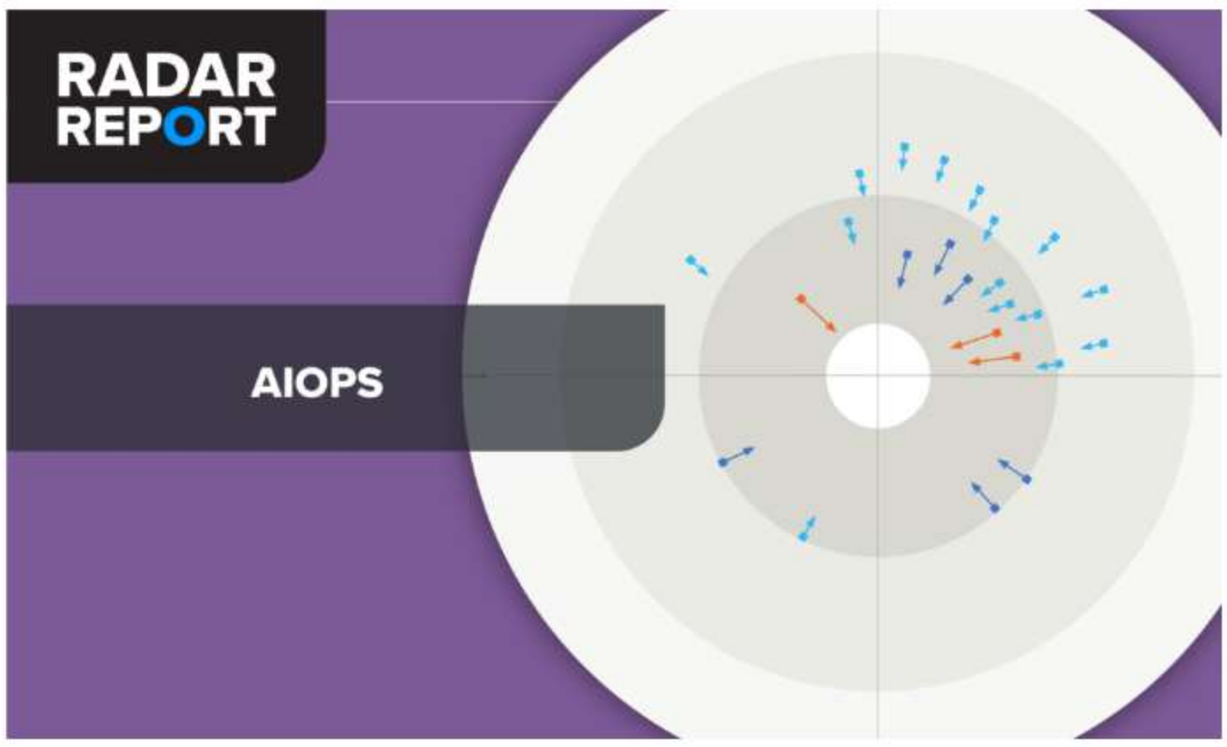

Ron Williams
Jun 14, 2022 – Market Radar

GigaOm Radar for AIOps Solutions v3.01

Taking Operational Awareness to the Next Level

Table of Contents

1. Summary

The last year proved to be one of explosive growth in AIOps tooling and solutions. Since our 2021 Radar report on AIOps, more vendors have added to the proliferation of AIOps solutions. In some cases, AIOps functionality was achieved by bolting an artificial intelligence and machine learning (AI/ML) engine to existing software, via acquisition or internal development, and marketing it as an AIOps solution. Other vendors built entire platforms around homegrown or acquired AI/ML, jumping into a crowded arena competing with pure AI/ML solutions and platform tools.. The market is still segmented into platform players, in which AIOps is one part of a platform of solutions, and other vendors who concentrate on AI while ingesting data from any source. Innovation continues as new vendors push AIOps to the edge of the enterprise.

The key functionality and evaluation metrics we assess demonstrate the realities of a growing vendor landscape and the need to differentiate vendors for enterprises seeking to take advantage of the power an AIOps tool can bring.

This year we're distinguishing AIOps solutions that require displacing existing tools from those that can be added to the IT tool box without major disruption. Often this dichotomy divides solutions into domain-agnostic and platform solutions. The domain-agnostic solutions can be added to any environment with minimal interruption of the business, while platforms may require the displacement of several existing monitoring solutions. In smaller organizations, displacing the existing monitoring tools is less of a concern because there has been less chance for siloed and homegrown solutions to take root. Typically, large enterprises already have tools for application performance management (APM), infrastructure monitoring, network monitoring, log management, development, and more, so replacing them can be challenging.

Auto-remediation of issues is a more important criterion than in previous reports. IT organizations have turned to automation to address the needs of operations teams. Whether as a distinct part of the AIOps solution or as a hand-off from AIOps, the ability to remediate problems discovered by the power of AI/ML emphasizes the ability of AIOps to do more without the need for additional staff.

AIOps solutions can return the cost of implementation and deployment quickly by reducing the number of operational personnel (or at least not requiring additional headcount) and delivering responses to incidents more quickly.

In the accompanying GigaOm report, "Key Criteria for Evaluating AIOps Solutions," we list the major features and evaluation metrics that should be applied when selecting an AIOps solution. In this report, we analyze the leading solutions in the market, weigh the key criteria and evaluation metrics used to assess them, and identify important technologies to consider for the future.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding, consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

To better understand the market and vendor positioning (**Table 1**), we assess how well solutions for AIOps are positioned to serve specific market segments.

- **Small-to-medium business (SMB):** In this category we assess solutions on their ability to meet the needs of organizations ranging from small businesses to medium-sized companies. Also assessed are departmental use cases in large enterprises, where ease of use and deployment are more important than extensive management functionality, data mobility, and feature set.
- **Large enterprise:** Here offerings are assessed on their ability to support large and business-critical projects. Optimal solutions in this category will have a strong focus on flexibility, performance, data services, and features to improve security and data protection. Scalability is another big differentiator, as is the ability to deploy the same service in different environments.
- **Managed service provider (MSP):** MSPs are enablers that take over a customer's network operations and deal with maintenance, upgrades, and other day-to-day activities. Their needs may align with those in the above categories, and solutions are assessed on ability to meet them.

In addition, we recognize three deployment models for solutions in this report:

- **Software as a service (SaaS):** These solutions are available only in the cloud. Often designed, deployed, and managed by the service provider, they are available only from that specific provider. The big advantages of this type of solution are the integration with other services offered by the cloud service provider (functions, for example) and its simplicity.
- **Customer-managed:** These solutions are meant to be installed by the customer, supporting deployments both on-premises and in the cloud, allowing the customer to build hybrid or multicloud solutions. They are more flexible, usually giving the end user more control over resource allocation and tuning across the entire stack. These solutions can be deployed in the form of virtual appliances, or as a traditional software component that can be installed on virtual machines or containers, and managed using Kubernetes.
- **Hybrid:** These solutions are meant to be installed both on-premises and in the cloud. They are more flexible, the administrator usually has more control over the technology stack, and they may be easier to conform to compliance or business requirements.

Table 1. Vendor Positioning

	MARKET SEGMENT			DEPLOYMENT MODEL		
	SMB	Enterprise	MSP	SaaS	Customer-Managed	Hybrid
BigPanda	+++	++	++	++	-	-
BMC	++	+++	++	++	++	-
Broadcom	++	+++	++	++	++	++
Centerity	+	+++	++	-	++	++
Cisco	++	+++	++	++	++	++
CloudFabrix	++	++	++	++	+++	++
Datadog	++	+++	+	+++	-	++
Digitate	++	+++	+	+++	++	++
Dynatrace	++	+++	++	++	++	++
Elastic	++	++	-	++	++	-
IBM	++	+++	++	-	++	-
Interlink	++	++	++	+	++	++
Logz.io	++	++	++	++	-	-
Micro Focus	++	+++	++	++	++	++
Moogsoft	++	+++	++	++	+++	-
Nastel	++	+++	++	+++	+++	++
New Relic	++	+++	-	++	-	-
OpsRamp	++	++	+++	++	-	-

PagerDuty	++	++	++	++	–	–
ScienceLogic	++	+++	++	++	++	++
ServiceNow	++	+++	–	++	+	–
Splunk	++	+++	++	++	++	+++
Sumo Logic	++	+++	++	++	–	–
Zenoss	++	+++	++	++	++	–

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2022

3. Key Criteria Comparison

Building on the findings from the GigaOm report, "Key Criteria for Evaluating AIOps Solutions," **Table 2** summarizes how each vendor included in this research performs in the areas we consider differentiating and critical in this sector. **Table 3** follows with insight into each product's evaluation metrics—the top-line characteristics that define the impact each will have on the organization. The objective is to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the market landscape, and gauge the potential impact on the business.

Table 2. Key Criteria Comparison

	KEY CRITERIA							
	Automation	Learning Systems	Dashboard & Reports	Data Consumption	Cloud Monitoring	Systems Integration	OpenTelemetry Utilization	OpenTelemetry Contribution
BigPanda	+++	+++	+++	++	+++	++	–	–
BMC	+++	+++	++	++	+++	++	++	+
Broadcom	++	++	++	+++	++	+++	++	–
Centerity	++	+	+++	+++	+	++	+	–
Cisco	+++	++	+++	+++	++	+++	+++	++
CloudFabrix	++	+++	++	+++	++	+++	++	+
Datadog	+++	++	+++	+++	+++	+++	+++	++
Digitate	+++	+++	+++	++	+++	+++	+	–
Dynatrace	++	+++	+++	++	+++	+++	+++	+++
Elastic	++	++	++	++	++	++	++	+
IBM	++	+++	++	++	++	+++	++	+
Interlink	+++	++	+++	++	++	++	+	–
Logz.io	++	+	++	++	+++	++	++	+
Micro Focus	+++	+++	+++	+++	++	+++	–	–
Moogsoft	++	+++	+++	+++	++	+++	++	–
Nastel	+++	++	+++	+++	++	++	+	–
New Relic	++	++	+++	++	+++	+++	++	++
OpsRamp	+++	++	++	++	+++	+++	+	–
PagerDuty	++	++	++	+++	+++	+++	++	–
ScienceLogic	+++	++	+++	+++	++	+++	–	–
ServiceNow	+++	+++	+++	++	++	+++	+++	++
Splunk	+++	+++	+++	+++	+++	++	+++	+++
Sumo Logic	++	++	++	+++	+++	+++	+++	+++
Zenoss	++	+++	++	+++	+++	++	+	–

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2022

Table 3. Evaluation Metrics Comparison

	EVALUATION METRICS					
	Flexibility	Manageability	Ease of Implementation	Usability	Security Integration (SSO, SOAR, SIEM)	Tool Displacement
BigPanda	+++	+++	+++	++	++	+++
BMC	+++	++	+++	+++	++	++
Broadcom	+++	+++	++	++	++	+++
Centerity	++	++	++	+++	+++	+++

Cisco	+++	++	++	++	++	++
CloudFabrix	++	++	++	++	++	+++
Datadog	+++	+++	++	++	++	+
Digitate	++	++	++	++	++	+++
Dynatrace	+++	+++	++	++	++	+
Elastic	++	++	++	++	+++	++
IBM	++	++	++	++	++	++
Interlink	++	++	++	++	++	+++
Logz.io	++	++	++	++	++	++
Micro Focus	++	+++	++	++	+	+
Moogsoft	+++	+++	++	++	+++	+++
Nastel	++	++	++	++	++	+++
New Relic	+++	+++	++	++	++	++
OpsRamp	++	++	++	++	++	++
PagerDuty	+++	+++	+++	++	++	+++
ScienceLogic	+++	++	++	++	+	++
ServiceNow	++	++	+++	++	++	+
Splunk	+++	++	++	++	++	+
Sumo Logic	++	++	++	++	++	+
Zenoss	++	++	++	++	++	+++

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

By combining the information provided in the tables above, the reader can develop a clear understanding of the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—balancing Maturity versus Innovation, and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.

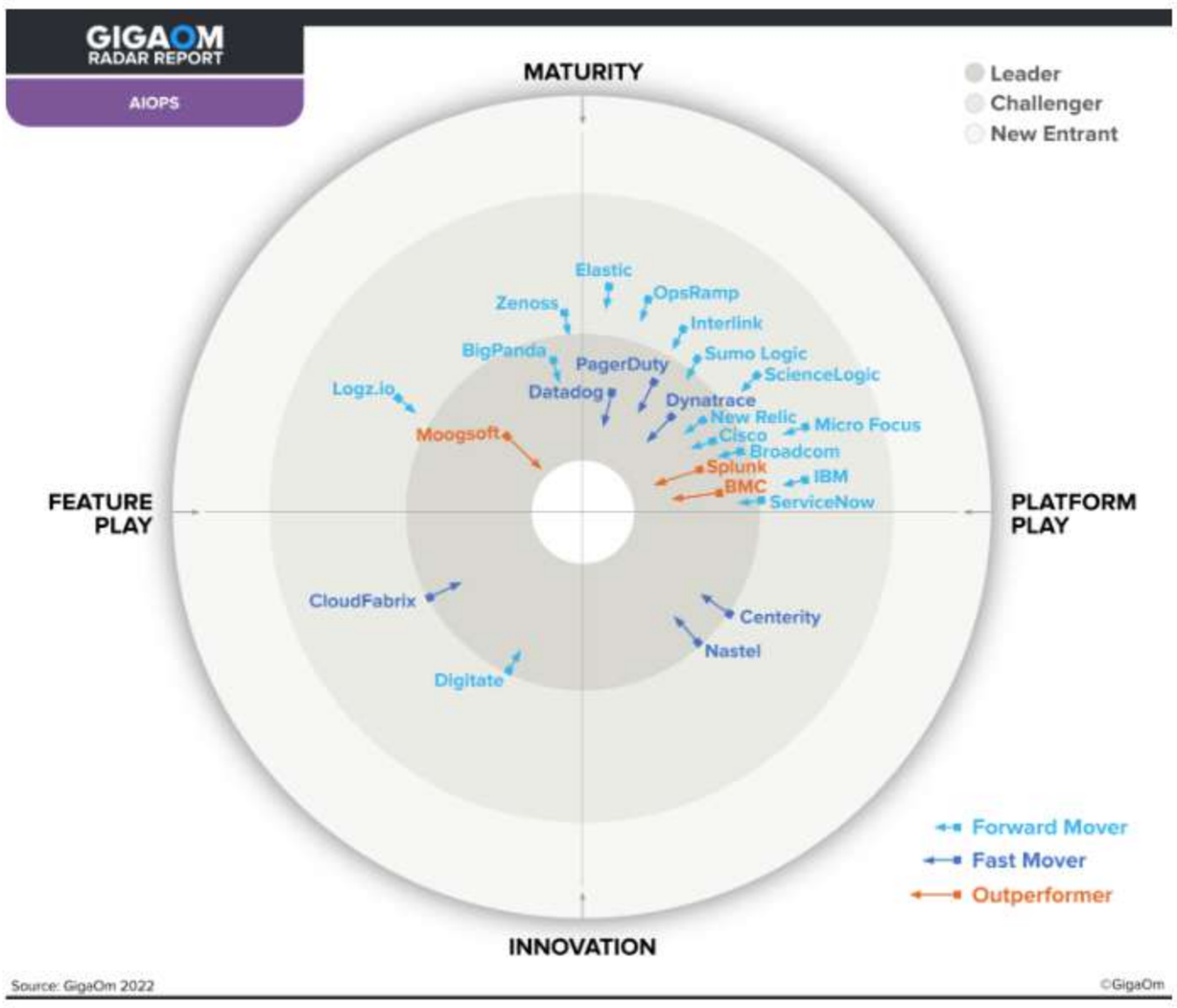

Figure 1. GigaOm Radar for AIOps

As you can see in the Radar chart in **Figure 1**, AIOps is dominated by Mature Platform-Play companies, followed by Mature Feature-Play (usually open-source) offerings.

Beginning at the top right, Mature/Platform-Play quadrant at 3 o'clock and moving towards noon, we see vendors known for having a complete package of tools for AIOps, which often includes mainframe and cloud management abilities. Many of these vendors are all-or-nothing suppliers; however, some now allow more flexibility in their offering. Even so, their marketing lends itself to a complete replacement of all IT operations management tools (ITOM). Any enterprise currently working with one of these vendors should review that

vendor's AIOps solution first.

As we move to the area between 2 o'clock and noon in the Maturity/Platform-Play quadrant, we encounter vendors who may have started as APM or log management tool providers and then crafted AI/ML into their offerings. These solutions may require the displacement of some existing monitoring tools. They strive to find a balance between displacing a few tools and installing a complete AIOps solution. In most cases, their previous setup can provide strengths in some areas, but probably won't suffice for every AIOps use case.

Vendors closer to the vertical, on either side of the line, are likely to require only minimal tool displacement. Some require no displacement at all while others may need to replace only a single tool. Enterprises keen to keep as many incumbent tools in place as possible should focus on this section of the Radar.

The majority of vendors in the top left, Mature/Feature-Play quadrant,displace no tools. They consume data from current tools, and integrate with existing systems. AIOps tools that take in external data only may be limited in the level of detail they can display; however, single-focused AIOps solutions often have integrations that allow them to display data more granularly. This portion of the Radar has the best options for enterprises looking for minimal or no tool displacement.

Finally, looking below the horizontal line, we see vendors with unique or innovative solutions for AIOps. Enterprises looking at these solutions will benefit from close examination of these inventive solutions for fit and purpose.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.

The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

BigPanda AIOps Event Correlation and Automation Platform

BigPanda—headquartered in Mountain View, California with offices in London, UK, and Tel Aviv, Israel—is developing a global market for its AIOps event correlation and automation platform that operates across the entire IT incident lifecycle. The platform comprises event correlation, root cause analysis, and Level-0 automation, and was built from the ground up to cater to the needs of complex IT environments. Using ML, it manages IT alerts and data coming out of the data center, and automates previously manual tasks, leaving engineers free for more strategic work. Fortune 500 enterprises such as Intel, Cisco, United, Nike, Marriott, and Expedia are among its customers.

One of the stronger features of the BigPanda solution is its proprietary AI/ML technology, Open Box Machine Learning, which uses a combination of supervised and unsupervised ML algorithms, deploying techniques such as word embedding, clustering, and convolutional neural networks. As the IT environment evolves and new data is ingested and correlated, Open Box Machine Learning suggests new correlation logic.

Open Box Machine Learning can automate much of the incident management lifecycle including correlation, problem detection, root cause analysis, prioritization, sharing, routing, and remediation. BigPanda's automation capabilities are good, but the handling of onsite resource data could be improved to limit the amount of data sent to the SaaS platform.

BigPanda's Level-0 automation includes workflow automations such as remediation, ticketing, notifications, and war-room creation. Enterprises can connect to third-party runbook automation tools to run workflows that are able to resolve incidents faster.

Strengths: BigPanda does not displace existing tools and brings AI/ML with strong analytics to the table. The solution's flexibility, dashboards, and cloud monitoring capabilities are good, adding up to a very manageable platform.

Challenges: BigPanda's consumption and integration of onsite data can be improved to make the process more easily implemented. BigPanda does not consume data from OpenTelemetry sources, nor do they contribute to OpenTelemetry. Go-live times could be faster, especially for enterprises with large onsite footprints.

BMC AIOps Platform

BMC products help companies become autonomous digital enterprises, with an emphasis on automation. Its portfolio provides technology and services for intelligent automation and service management, enterprise DevOps, mainframe modernization, IT optimization, and security and compliance. BMC Helix Operations Management with AIOps supplies its AIOps capabilities. BMC claims to work with 86% of the Forbes Global 50 and customers and partners around the world. The company is headquartered in Houston, Texas, and has 66 offices in 39 countries.

The BMC AIOps platform consists of three individual products: BMC Helix Operations Management with AIOps, BMC Helix Discovery, and BMC Helix Continuous Optimization. The platform targets midsize and large organizations and supports both traditional on-premises and cloud-based systems. This heterogeneous support using a single set of tooling and interfaces not only helps existing BMC customers leverage their investments, it also moves new BMC customers to the AIOps platform. Cloud deployments are growing compared to on-premises installations, due to the many advantages offered by SaaS, especially lower cost of ownership.

BMC Helix is a platform with a single data model that shares core and common services, such as ingestion, single sign-on (SSO), AI/ML analytics, and visualization. It's available in the BMC private cloud, Amazon Web Services (AWS), and several regional private clouds, and is expected to expand to other public clouds later this year.

BMC's solution is very flexible. When implemented onsite, all enterprise hardware and software are covered completely. The SaaS offering can consume data from onsite via collectors and other tooling, though the amount of data sent to it should be monitored to control costs. The SaaS implementation is considered to be easy. The BMC licensing model is by endpoint, not data ingestion. BMC has a standard retention policy and no additional costs for volumes of most data, with the exception of logs, for which they have a storage limit and the option for customers to purchase additional capacity.

BMC can implement portions of Helix for those not ready to take on the entire platform. However, the intent is that BMC will eventually become a company's monitoring tool of choice, with its AI providing operational awareness.

BMC continues to enhance integration when implemented onsite with cloud-based systems. This includes both integration via StreamWeaver as well as direct integration of those cloud sources. Enhancements over the past year include support for application programming interface (API)-based discovery of public cloud assets, with more advanced support of AWS SSM and AWS Organizations, as well as Google Cloud Platform (GCP) IAP support. Helix supports API-based export of data from the platform for use with third-party tools.

Strengths: The BMC platform for AIOps is comprehensive and has strong capabilities for monitoring the entire enterprise. BMC can consume OpenTelemetry data and it contributes to the open-source effort. Flexibility has improved over last year's offering, along with cloud monitoring. Implementation of the entire BMC platform is not a prerequisite to using the AIOPs portion of the platform.

Challenges: The entire BMC platform is designed to displace existing tools in an enterprise, and some enterprises may find it difficult to accept the level of change needed to embrace the entire platform. (Note that even the more piece-by-piece implementation that's available has the same ultimate goal.) The perception that BMC is only for large onsite enterprises has diminished with the latest Helix releases, especially the SaaS offering. Third-party systems may have difficulty mining BMC's datastores, even though the API has improved. This may be an issue for security groups that need that content.

Broadcom

Established more than 60 years ago, Broadcom Inc. is a global infrastructure technology company with roots in the technical heritage of AT&T/Bell Labs, Lucent, and Hewlett-Packard/Agilent. Acquisitions have brought together Broadcom, Broadcom Corporation, LSI, Brocade, California Technologies, and Symantec to provide semiconductor and infrastructure software solutions. Broadcom is headquartered in San Jose, CA, with offices across 25 countries globally.

The DX Operational Intelligence AIOps platform from Broadcom Software correlates data across users, applications, cloud-native architecture, hybrid infrastructures, and network services, and applies ML, advanced analytics, and automation to deliver a new level of visibility and data-driven insights. It makes data actionable by providing comprehensive insights across the digital delivery chain, and it can drive continuous improvement to speed service delivery, increase IT efficiency, and accelerate innovation. With this solution, operations teams can optimize service levels, operations, and business outcomes.

The solution also offers full-stack observability into the digital experience (mobile, web, crash, journeys, funnel), app-to-network monitoring, and support for cloud-native architectures (lambda, open tracing), while aligning with third-party data-to-business services with measurable KPIs to help prioritize issues and relate performance to business goals as organizations seek to transform the customer experience.

Broadcom Software uniquely leverages its deep domain expertise in network, application, and infrastructure to correlate silo problems to the broader digital ecosystem. Enterprises can therefore choose to displace all tools or to add AIOps functionality to their existing tool set.

Broadcom Software provides support for all levels of the enterprise, including full-stack observability for public and private clouds.

Broadcom Software provides good flexibility, not just in the deployment of the solution, but in the day-to-day manageability of the solution.

Strengths: Broadcom provides an extensive platform for AIOps that spans from mainframe to cloud computing. The ability to be either a platform or an add-on to an existing environment is a plus.

Challenges: Broadcom does not contribute to OpenTelemetry. Implementation could be easier.

Centerity AIOps

Centerity is headquartered in Newton, Massachusetts, with an R&D center in Israel. Its AIOps platform, which has been deployed more than 300 times since 2010, is focused on providing visibility, context, and control at the edge, which, it believes, is missing from many solutions. It calls its approach to supporting the edge CSM^2 (Connect-Secure-Monitor-Manage). The company targets a number of sectors, including retail and hospitality, financial services, healthcare, manufacturing, energy and utilities, and the public sector. The company also has a strong practice in Radio Systems, Infrastructure for Public Safety, and Professional Communications.

Centerity is a single unified platform with all features and functionality provided as a software deliverable that can be deployed on a physical server or appliance, on-premises, in the cloud, or in a hybrid architecture model. There is no SaaS version available. Some capabilities are based on third-party features, but they are all fully integrated to the platform via an OEM relationship and stay within Centerity's responsibility and control. Centerity shines in real-time system performance analytics for industries with complex operating environments, particularly at the edge of the enterprise. These environments generally have multiple data types from multiple data sources, and require monitoring and visibility across the entire environment. This heterogeneity typically includes non-standard distributed edge devices such as POSs, ATMs, and kiosks; and Android and iOS-based business edge devices.

There are some weaknesses in AI/ML and cloud monitoring and with systems integration. These are balanced by good usability and security integration. The unique edge AI/ML is innovative.

Centerity does not displace many existing tools because it provides monitoring and intelligence for additional devices not normally monitored. It has good security integration with SSO, security orchestration automation and response (SOAR), and security information and event management (SIEM) tools.

Strengths: Centerity provides an innovative entry to the AIOps world by focusing on edge devices and the intelligence to monitor them. The solution is easily managed and consumes data from any source, including OpenTelemetry data streams.

Challenges: Both AI/ML and cloud monitoring capabilities need improving. Bidirectional integration with other systems is a weak point. Centerity is not a contributor to OpenTelemetry.

Cisco (AppDynamics) Central Nervous System for IT

Founded in 1984 and headquartered in San Jose, California, Cisco is a multinational corporation, with over 35,000 employees in more than 115 countries. Its solutions provide the networking foundation for service providers, SMBs, and enterprise customers, which includes corporations, government agencies, utilities, and educational institutions.

With the acquisition of AppDynamics, Cisco provides a vision for AIOps: the Central Nervous System for IT—an AIOps platform that delivers cross-domain visibility and insights, along with the ability to automate actions, reduce time-consuming IT tasks, and enable teams to drive innovation.

Cisco (Appdynamics) can ingest data from its own agents as well as via open standards such as Prometheus and OpenTelemetry. It leverages a topology and dependency-aware data model that spans multiple domains. The solution has strengths in dashboards, reporting, and data consumption, and makes good use of OpenTelemetry.

The platform is well-suited to larger enterprises, though smaller companies can use it successfully as well. The deployment model is flexible, allowing both SaaS and customer-managed deployments.

As this solution is based on the APM framework of AppDynamic, there is excellent full-stack data available for troubleshooting and remediation, and as a Cisco product, it handles network devices well.

Cisco (AppDynamics) is moderate in its tool displacement, but the entire platform can replace a number of tools if that is preferred.

Strengths: This AIOps solution has good flexibility. It handles public clouds well and integrates with other solutions easily. It makes good use of OpenTelemetry and contributes to this open-source standard.

Challenges: Cisco is moving past the APM legacy of AppDynamics, but must still deal with the perception that it is an APM tool on steroids. Deployment in large enterprises may require professional services.

CloudFabrix

CloudFabrix was founded with the aim of enabling autonomous enterprises by adopting a “data-first, AI-first, and automate everywhere” strategy. Its Robotic Data Automation Fabric (RDAF) unifies observability, AIOps, and automation within a single SaaS platform (cfxCloud) built on CloudFabrix’s own cloud. The platform is built with microservices, is cloud native, and can run entirely in the cloud, in a hybrid deployment, or on-premises. The company is headquartered in Pleasanton, California, with an office in Stockholm, Sweden, covering EMEA, and another office in Hyderabad, India.

RDAF powers multiple services deployed on top of the AIOps platform, including Log Intelligence, Asset Intelligence, and Service Intelligence.

Unsupervised and supervised learning are both provided, along with topology detection with data models. Supervised learning is used in the Incident Room to detect possible root causes. On-demand and periodic training of ML models is initiated when new datasets are received or changes to existing datasets occur. Multiple ML training experiments can be performed using ML pipelines, and custom ML pipelines can be curated using a user interface (UI)-driven click-through experience for hyperparameter tuning, which uses a no-code approach.

Broad data integration is supported, with RDAF used to integrate data with new sources. Data can be consumed from the following ITOM systems for performance metrics: AppDynamics, Dynatrace, New Relic, Datadog, LogicMonitor, Zabbix, PRTG, Prometheus, Nagios, SolarWinds, NodePing, VMware vCenter, VMware vROps, Cisco Meraki, Cisco ACI, Cisco UCS Manager/Director, SNMP, e-mail-based alerts, CA/Broadcom UIM, Microsoft SCOM, IBM Tivoli Netcool, ITRS Geneos, and Dell EMC Smarts. In terms of IT operations management (ITOM) and SIEM, log data can be ingested from Splunk and Elasticsearch. Support is also provided for datastores and data lakes, IT service management (ITSM), configuration management database (CMDB), the collaboration platforms Slack, Microsoft Teams, and Twilio; and Terraform, Ansible, and Chef for automation. New this year is its Log Intelligence service.

The low-latency distributed data fabric allows cfxCloud to ingest, integrate, transform, and load data from or to any system. Once that data is within the platform, users can interact with and operationalize it using a set of more than 800 existing bots and create others via a self-service pipeline. Users are thus able to create low-code or no-code pipelines to implement customizable data integrations.

Strengths: RDAF provides a unique data fabric for ingesting data in any location. The ability to deploy the platform in any environment is a plus. The method for defining bots and the data pipeline is excellent. OpenTelemetry data ingestion is supported.

Challenges: The UI needs to provide a better overall experience and a better ability to deep-dive into problems. Though the UI is functional, others in this space provide more ease of use and a better ability to isolate problems. The company does not contribute to OpenTelemetry.

Datadog

Datadog was formed in 2010 to eliminate the friction that can occur between developers and system administrators. Its growth is driven by a focus on automation and real-time monitoring and security for cloud applications. Launched as an infrastructure monitoring company, Datadog has expanded its portfolio via both acquisition and organic growth to offer solutions throughout the full observability space. Headquartered in New York City, New York, it has regional headquarters in Boston, Dublin, Paris, Singapore, Sydney, Tokyo, and offices across the US, Europe, and Asia Pacific.

Datadog’s AIOps capabilities are powered by Watchdog, an algorithmic feature for APM and infrastructure metrics that automatically detects potential application and infrastructure issues. The AIOps features plug into existing Datadog telemetry to augment, accelerate, and automate user operations and workflows. Anomaly detection, forecasting, outlier recognition, data correlation, and dependency mapping are all available. Users have a choice of automated anomaly detection or forecasting and running either using a custom ML-based alert configuration.

Proactive anomaly detection and root cause analysis is provided by Watchdog, with users able to opt into receiving alerts. All alerts offer API and webhook integrations and they can be connected to SOAR and external management systems to automate runbooks and perform auto-remediation.

Datadog provides flexible dashboarding capabilities that allow users to create custom dashboards that can be shared both within the organization and publicly.

Datadog offers a complete observability suite that includes real-user monitoring, synthetic monitoring, APM, infrastructure monitoring, container monitoring, log management, network performance monitoring, continuous profiler, CI visibility, and database monitoring. This comprehensive observability allows Watchdog to causally connect end-user impact data with application failure data and detect root causes stemming from code and infrastructure issues.

Datadog provides more than 500 integrations, including to a wide range of private and public cloud services from major providers. Other integrations include ITSM, CMDB, continuous integration/continuous delivery (CI/CD), FinOps, security, and runbook automation tools. The availability of public APIs means that tools without a native integration can be manually integrated.

Full support is provided for OpenTelemetry, including the exporting and consumption of traces and metrics, support for the AWS OpenTelemetry distribution, and native support for Lambda OpenTelemetry.

Datadog displaces many existing tools. When considering this solution, strategic planning for tool change should be considered.

Strengths: Datadog is strong in the key criteria areas of automation, dashboards and reports, data consumption, cloud monitoring, systems integration, and OpenTelemetry utilization. There are strong root cause analysis abilities and good workflow integration. Additionally, Datadog offers insights at query time (when a dashboard or drill-down is executed). Onsite data can be sent to the SaaS engine.

Challenges: Datadog provides web crawlers and recurring API polling to obtain onsite data which may make gathering on-premises data more challenging. Best value is achieved by adding other ITOM tools. It also needs to increase its geographic footprint, which is currently limited to the US and EU, as this prevents customers in highly regulated industries in other regions from implementing Datadog because they are unable to send their data outside of their own country. There is no on-premises solution at this time.

Digitate

Founded in 2015, Digitate is headquartered in Santa Clara, California, with an office in Pune, India. Its platform, ignio, provides AIOps software for autonomous operations that takes a closed-loop approach to prevention and resolution of issues, combining context, insights, and intelligent automation. Customers include large global enterprises across various industry verticals. In addition to AIOps, ignio also comprises ignio AI.WorkloadManagement, ignio AI.ERPOps, ignio AI.Digital Workspace, ignio Cognitive Procurement, and ignio AI.Assurance. ignio AIOps creates a unified view of multicloud environments that includes the behavior profiles of systems and applications, providing visibility across AWS and Microsoft Azure cloud services.

ignio is a single, integrated SaaS-based platform that combines observability, blueprinting, enterprise application management, workload management, and end-user device management. The repository contains more than 10,000 out-of-the-box automations and prepackaged integrations for major IT standard tools. The solution manages an organization's data flow, both horizontally and vertically.

ignio manages business-critical technology lifecycle activities autonomously, without the need for human intervention. Integration with tools and systems is typically achieved using either exposed APIs from ignio or APIs exposed by other tools and systems.

ignio self-learns normal behaviors and is then able to identify patterns to detect deviations and anomalies in operational metrics and derive current thresholds. Time-series analysis techniques are used to capture changes, outliers, trends, and patterns to profile normal behavior of each blueprinted entity. Data about alerts, metrics, and dependencies is continually analyzed to learn about trends, patterns, correlations, forecasting models, fault propagation models, and fault-fix models. The solution is rule-based, model-based, and case-based.

Persona-specific dashboards and reports are provided across the value chain and include end user experience management, ERP/SAP operations, batch workload operations, application operations, infra operations, blueprint reports for end-to-end enterprise visibility, and governance reports. Dashboards and reports can be customized at the organization, business, or enterprise level, and they can be shared and exported.

Out-of-the-box integrations are provided to a variety of tools, and an extensible adapter framework allows ignio to integrate with ITSM, as well as with service desk, custom ticketing, monitoring and event management tools, and CMDBs. Both push- and pull-based integrations are supported.

Strengths: Digitate is strong in the key criteria areas of automation, learning systems, dashboards and reports, cloud monitoring, and systems integration. Its automation capabilities place it in the Innovation category of AIOps solutions in our Radar chart (**Figure 1**).

Challenges: Digitate's support for OpenTelemetry is weak, and it does not contribute to the project. Digitate needs to improve ignio to include support for GCP, which is on its roadmap, along with the ability to proactively manage potential incidents that occur as a result of change.

Dynatrace

The Dynatrace Software Intelligence Platform includes a full multi cloud observability platform, incorporating applications, APM infrastructure, and user experience, based on the company's proprietary Davis AI engine, as well as AIOps capabilities. Dynatrace adheres to the latest open-source standards, including OpenTelemetry.

Dynatrace is a single, full-stack platform that includes APM, AIOps, infrastructure monitoring, digital business analytics, digital experience management (DEM), application security, log analytics, and cloud automation for enterprise IT departments and digital businesses. Using automation in concert with the Davis AI engine, the Dynatrace platform provides root cause details regarding application performance, generates insights into the underlying infrastructure, and presents an overview of the user experience. Capabilities include continuous discovery, self-learning of optimal cloud and application behavior, and proactive anomaly detection prioritized by business impact. The system is designed to scale and operate in hybrid clouds, public clouds, or edge environments, as well as on-premises.

The platform is available via SaaS and managed delivery options. It is FedRAMP Moderate Impact Level authorized. Licensing is generally based on a consumption model for SaaS and managed (that is, distributed SaaS) deployment models. AIOps and business analytics are platform features and not subject to incremental charges.

PurePath is Dynatrace's patented distributed tracing and code-level analysis technology. It automatically integrates high-fidelity distributed tracing with user experience data, data from open-source technologies, and code-level—including OpenTelemetry— analytics.

Dynatrace has extensive learning systems capabilities that are based on three core technologies:

- OneAgent collects data and contextualizes it at the same time.
- PurePath combines distributed tracing with code-level visibility, topology information, and metadata. PurePath is automatically generated and can be extended with external data. ML is not required to discover dependencies from historical data because code-level insight delivered through agent-based byte-code injection is used directly to derive causality of dependencies between software modules. Smartscape autodiscovers and visualizes all of the topological dependencies across infrastructure, processes, and services and can be expanded. ML is used for automatic multidimensional baselining, which enables predictive analytics.
- Davis, Dynatrace's deterministic AI engine, is used to carry out anomaly detection and automated root cause analysis. It applies fault domain analysis to software and infrastructure monitoring and to AIOps.

Dynatrace provides customizable dashboards and reports, which can show both strategic and tactical data. It includes preconfigured and customizable visualizations for various use cases and user types out-of-the-box. Dashboards consist of tiles that are flexible and can be configured and arranged to fit specific requirements. Many prefigured and configurable tiles are provided, and dashboards as code can be shipped with the service as part of the CI/CD pipeline.

Network device monitoring is limited to simple network management protocol (SNMP). In large enterprises, SNMP management of a diverse network device population may prove difficult. Dynatrace does not support ingestion of native network NetFlow or Probe-based monitoring systems.

OneAgent can now be used at a reduced cost to monitor only the infrastructure, removing a concern with last year's offering.

Strengths: Dynatrace is strong on learning systems, dashboards and reports, cloud monitoring, systems integration, and OpenTelemetry utilization. Initial deployment is relatively easy and Dynatrace provides an excellent full-stack view of applications. The Davis AI engine is included for all customers.

Challenges: This implementation of Dynatrace can be complex, especially when the Dynatrace OneAgent cannot be deployed. Day-to-day management of Dynatrace may require a long learning curve in large environments. Interviewed users describe the implementation as heavily dependent on rules to match business logic and company specific workflows, which can require a fair amount of configuration and testing, adding to implementation time. Dynatrace displaces many existing tools, and should be evaluated based on a strategy of change.

Elastic

Headquartered in Mountain View, California, with offices throughout North America, EMEA, and Asia Pacific, the company name is "Elastic." The company was founded in 2012, filed for IPO in June of 2018, and listed on the NYSE in October 2018. In 2015, it was rebranded Elastic, following the combination of three open-source tools—Elasticsearch, Logstash, and Kibana—to create the ELK Stack. Elastic provides enterprise search, observability, and security solutions, with a customer base that includes Netflix, Uber, Slack, and Microsoft. In 2017, Elastic joined forces with Opbeat, a Copenhagen-based APM company, and in the same year, it acquired Optimyze to help with observability. Other acquisitions include Prelert for ML, Found forCloud, and Endgame, Cmd, and build.security to help with security.

Elastic Observability is used in Elastic's AIOps solution. The product ingests metrics, logs, and traces from applications hosted in a data center or in AWS, Azure, or Google Cloud environments. All business and operational data is ingested using Elastic Integrations, which provides support for open standards and open-source projects such as OpenTelemetry, Jaeger, and Prometheus.

Search, drilldown, pivoting, and visualizations are available, as is automated analysis through alerting and ML-driven anomaly detection across all data, which enhance understanding of correlation and causation across telemetry data.

Elastic has good AI/ML capabilities and appears to be centered around correlating anomalies to downstream data and dependencies to assist with root cause analysis. There are two unsupervised model types, anomaly detection and outlier detection. Anomaly detection runs continuously and creates a probability model to identify unusual events. Outlier detection, which does not run continuously, identifies unusual points in a dataset by analyzing a point's proximity to similar data points, and the density of the cluster of points around it.

The ML engine is data-agnostic and can be used to support data that's being ingested by finding anomalies and outliers and producing forecasts based on trends.

Elastic is strong on security integration, by which operations and security teams can be unified on a single platform to monitor application and infrastructure performance. Built-in SIEM and endpoint security are included. The Elastic platform provides mitigation, detection, and response, with ML and behavior analytics available to detect and react to threats.

There are self-managed and SaaS offerings. Pricing is based on the use of resources, with the cost determined by hardware resources used to store, search, and analyze the data, regardless of the use case or deployment model.

Strengths: Elastic has good capabilities across the key criteria areas of automation, dashboards and reports, data consumption, cloud monitoring, systems integration, and OpenTelemetry utilization.

Challenges:. Elastic struggles with identity. Given its previous background in log management and APM, determining the best fit for Elastic is difficult. They have no poor evaluation criteria, but also do not stand out against the large number of vendors in the market. As has been pointed out, Elastic is the basis for other AIOps players in this Radar.

IBM Cloud Pak for Watson AIOps

IBM provides AIOps and IT automation solutions, but it requires a number of products to create a complete solution. IBM Observability by Instana APM provides full-stack observability; IBM Turbonomic Application Resource Management provides dynamic resource provisioning; and predictive AIOps is enabled through IBM Cloud Pak for Watson AIOps. Sources across local, hybrid, and multi cloud environments can be managed. The core components of the solution include event management, incident diagnosis, incident resolution, and insight delivery, and there's an ecosystem of connectors and capabilities for managing all aspects of the AIOps lifecycle, including model training and execution.

IBM Cloud Pak for Watson AIOps supplies prediction and communication capabilities, and it enables the resolution of IT events by applying AI to structured and unstructured data from applications and infrastructure components of the entire IT stack. ML models are trained to read and analyze logs, events, and other incident data to discover and correlate anomalies. A ChatOps interface allows the models to present insights to help users understand the issue and advise on resolutions.

A strength for IBM is the embedding of Watson AI in IBM Cloud Pak for Watson AIOps, which ships with prebuilt and tested ML models and includes the ability to derive insights from unstructured data. ML and advanced topological analytics can be used to automatically consolidate and organize events into actionable incidents. The ML engine is trained to recognize a healthy baseline, and using that, it can then detect anomalies. Using relevant context, the probable cause can be determined, and an automated response initiated.

Each IBM Cloud Pak is powered by common AI and automation components that include process mining, task mining, RPA, a unified asset repository, and a single event hub to process event data in real time and provide data to train the ML engine. IBM deploys natural language processing (NLP) and deep learning models to provide risk predictions.

Hundreds of out-of-the-box integrations are available across local, hybrid, and multicloud environments. APIs provide integration to thousands of other solutions, and IBM also claims to support integration to in-house-built applications via webhooks, email, and SNMP.

IBM Cloud Pak for Watson AIOps is customer-managed. As it is a modular solution, it does not have to displace existing tools.

Strengths: IBM has outstanding capabilities in learning systems and systems integration, and good capabilities in the other key criteria.

Challenges: Although IBM utilizes OpenTelemetry data, it does not contribute to the project; however, participation is on its roadmap.

Interlink Software

Interlink Software, which is headquartered in Wilmslow, Cheshire, UK, with an office in Orlando, Florida, was founded in 1996. The company provides a unified AIOps platform, using end-user, incident, and performance data, and metrics from any source. This is an onsite, cloud-based, or hybrid solution with desktop and mobile applications that combines ML and integration capabilities to provide actionable insights. Its platform comprises a number of components—Service Visualization, Hybrid IT Infrastructure Monitoring, IT Workflow Automation, and the Incident Alert Management App.

Interlink Software has drag-and-drop functionality that lets users build consistent and reliable automations for multicloud and multiple platform environments. Additionally, its built-in ML offers self-healing remediation, pattern recognition, root cause analysis, and predictive analytic capabilities. End users can build and maintain workflow automations to accelerate operational processes and provide consistent service availability.

The platform uses unsupervised (unattended) and supervised (attended) ML algorithms. The unsupervised (or unattended) bots work independently. Under predefined conditions, they are triggered automatically to execute tasks, which are governed by preset logic and rules, and authorized via allow-list protocols. Supervised (or attended) bots are maintained by ITOps staff. Operators manage the orchestration of the required tools to implement the most efficient incident resolution.

Automated reporting capabilities track metrics and events both in real time and historically for any service. Early indicators of operational targets or service level agreements (SLA) breaches are supported within the platform. End users can baseline service reports month-to-month to provide consistent service.

Customizable dashboards provide views of high-level status, business outcomes, system component status, application status, service changes, and service incidents. All of the dashboards can integrate with common application and infrastructure monitoring tools, as well as change management and security tools.

Flexible data consumption is provided with a growing number of out-of-the-box integrations to popular applications, networks, infrastructures, logs, and service desk and service management tools. Legacy in-house-developed open-source tools can be integrated through open API support using Logfile Listener, SNMP v2/v3, TCP Listener, UDP Listener, Database, and Web Services (REST, SOAP, Webhook).

Interlink supports integration via OpenTelemetry APIs and software development kits (SDKs).

Strengths: Interlink Software has outstanding capabilities in automation and dashboards and reports. It has a good level of functionality across the other key criteria.

Challenges: The company does not currently contribute to OpenTelemetry; however, future contribution is under review.

Logz.io

Logz.io is an Israeli-based company with a large presence in the US. It primarily uses open-source technologies and open standards (such as OpenTelemetry) to monitor, log, collect, search, and analyze observability data. Logz.io Insights combines ML algorithms with human knowledge to identify and contextualize issues to help enterprises with AIOps tasks. The vast majority of its revenue comes from its observability platform. Logz.io works well with agile, cloud-native customers, most of whom are running Kubernetes in production. The company has more than 1,300 customers, including Siemens, Unity, and ZipRecruiter.

Logz.io is a SaaS-based observability and security analytics platform that's based on leading open-source technologies. It provides full visibility into cloud infrastructures and applications, enabling users to unify and visualize logs, metrics, and traces to monitor the entire cloud infrastructure and correlate data to investigate issues. A cloud SIEM solution is also offered to provide security. Observability data can be organized into dedicated environments for each team, and noisy data is eliminated. The platform includes AI/ML capabilities that automatically enable the ingestion of any amount of observability data for storage and analysis without the need for human intervention. ML-assisted noisy data recognition is available with Data Optimization Manager,

which identifies data that is not required, allowing engineers to remove it.

Cloud monitoring capabilities are strong, as is expected in a cloud observability platform. Integration with all key services from cloud providers is available, including AWS CloudWatch, Azure Monitor and Azure Application Insights, and Google Cloud Operations Suite. Users are able to configure a template to launch a serverless function that forwards data from these cloud services to Logz.io at customer-defined times to provide real-time metrics. Logs can also be retrieved from these tools and Logz.io can establish trace IDs based on the information in the logs.

While Logz.io does make use of a learning system for training its ML engine, this is a weak area for the vendor as its capabilities are not as advanced as those of its competitors. The solution makes use of user input training and automated reinforcement training over time. Its Cognitive Insights combine ML and crowdsourcing as another method of problem identification and to connect the issues with actionable information that can be implemented for resolution.

Strengths: An area of particular strength for Logz.io is its cloud monitoring capabilities. It is also strong on automation, dashboards and reports, data consumption, systems integration, and OpenTelemetry utilization.

Challenges: The weakest area for Logz.io is its learning systems capabilities. Contributions to OpenTelemetry are attributed to its CTO. As a SaaS-only offering, support for onsite infrastructure is weaker than that of others.

Micro Focus

Micro Focus is one of the longest-running players in the ITOM monitoring space. Founded in 1976, the company has a long history of building out its technology stack and providing solutions for the DevOps, hybrid IT, security and risk management, and predictive analytics markets. Micro Focus offers a full AIOps solution with automated discovery, monitoring, and remediation in either a SaaS or on-premises deployment.

Its Operations Bridge monitors IT environments, consolidating and normalizing data from third-party tools. Automated discovery, monitoring, analytics, and remediation are applied to data across traditional, private, public, multicloud, and container-based infrastructures. This is a single product with multiple modules that can be selected based on requirements. Micro Focus's OPTIC platform, which provides a single data lake for the rapid ingestion of data to support real-time analytics, as well as other capabilities such as containerization, is an integral part of its solution.

An automation tool is included that has thousands of out-of-the-box operations and a drag-and-drop workflow builder. For users who need to access existing work, it can call other automation tools, such as Ansible. A large number of APIs and command line interfaces (CLIs) are published and documented, allowing customers to ingest and consume data, and configure and execute functionality programmatically from external applications. Integration with multiple ITSM ticketing solutions is available.

One of the areas that is automated is monitoring in that Operations Bridge detects when new resources are made operational and starts monitoring based on a predefined template for the particular type of resource. Collectors are provided for a great many data sources, but the solution also integrates with customers' third-party tools.

AI/ML is used extensively throughout the product, with both supervised and unsupervised ML used. The underlying training and ML optimizations have been automated. Users are able to customize the algorithms to meet specific requirements.

Micro Focus provides out-of-the-box reports and templates, and users can create their own reports using Visio. The company publishes its schema, allowing users to use their own business intelligence (BI) tool of choice. Micro Focus also supports DevOps processes with dashboards-as-code. Tailored dashboards show key status, business, and IT KPIs, and the solution provides consolidated performance and event management, optimization, and customizable dashboards.

Strengths: Micro Focus is particularly strong in automation, learning systems, dashboards and reports, data consumption, and systems integration.

Challenges: Micro Focus currently does not support or contribute to the OpenTelemetry standard, something it recognizes is a limitation. It is currently working on providing support for OpenTelemetry data.

Moogsoft

Founded in 2012, Moogsoft has more than 200 customers worldwide, including American Airlines, Fannie Mae, Fiserv, Fox, Uber, and Yahoo!. It has strategic partnerships with leading MSPs and outsourcing organizations including AWS, Cisco, HCL Technologies, TCS and Wipro. The Moogsoft AIOps platform is a cloud-native observability product targeted at DevOps pros and site reliability engineering (SRE) teams. It provides intelligent noise reduction, alert correlation, and native observability capabilities, including metrics collection and anomaly detection. Also included are workflows and integrations with notification and alerting tools. The Moogsoft platform is available on-premises, hosted via a cloud services provider, or as a cloud-native SaaS application. It's API-first, and customers are able to solve many problems and challenges programmatically.

Learning capabilities are one of the strengths of the Moogsoft offering. Multiple ML techniques are applied depending on the requirements. Unsupervised ML is used in entropy calculations and similar situations, while similarity clustering uses semi-unsupervised ML. Supervised ML is used for probable root cause because it is neural network-based. Moogsoft also uses Graph Theory and NLP techniques. For example, when data items coming from different sources are not consistent, Moogsoft uses NLP-based similarity algorithms to correlate data into a single incident. Moogsoft has more than 70 patents to support its many ML algorithms. Advanced algorithms are used for pattern discovery and significance testing.

The product includes basic dashboards for all solutions. Comprehensive reporting is provided via Grafana for both on-premises and hosted solutions. Daily insights are currently provided for the SaaS solution.

Data ingestion is another strength for Moogsoft, which offers comprehensive support for leading third-party tools in cases where it's unable to digest data natively, and it has open event and metric APIs to enable ingesting data directly from the source. In addition, it supports custom integrations.

Moogsoft integrates with external solutions such as CMDB, ITSM, and CI/CD systems. In many cases, the integration is bidirectional. As the solution of engagement, Moogsoft often provides an automated workflow to tie these systems together.

Moogsoft's workflow engine provides a low/no-code method for customers to ingest, enrich, and correlate data, allowing them to collaborate and automate the lifecycle of an incident.

Moogsoft scores well with regard to tool displacement. As it consumes data from any source, the need to replace existing tools is minimal.

Strengths: Strengths for Moogsoft are its learning systems, dashboards and reporting, data consumption, and systems integration capabilities. It's a flexible solution that enhances manageability and provides a good level of security integration.

Challenges: There's currently a lack of parity between the on-premises and SaaS versions of the solution. For example, the on-premises platform contains some advanced features not available in the SaaS version. However, due to its cloud-native architecture and CI/CD and DevOps culture, features are being added to the cloud platform faster than to the on-premises version. Moogsoft needs to ensure parity in the functionality of the two versions.

Nastel XRay The Nastel Platform

Founded in 1994 by CEO David Mavashev and headquartered in Plainview, New York, Nastel Technologies provides IT organizations and business executives with the tools and insights they need to understand and manage their digital environments. Customers include large banks, financial services, insurance providers, retail chains, transportation, and manufacturing companies. Solution capabilities include integration infrastructure management, middleware management, managed file transfer, transaction tracking, cloud migration, and hybrid cloud.

Nastel XRay and the Nastel platform take the configuration information and message content of messaging middleware integrations to create a topology view of a transaction across the entire application stack, overlaying it with performance data from each system. This allows each user transaction to be compared to the historical record using ML to discover anomalies and to enable root cause analysis. Enterprises can extract critical information and insights from the middleware layer and combine it with other relevant data to enable 360-degree situational awareness for enterprises that use IBM MQ, IBM IIB (IBM Integration Bus), IBM ACE (App Connect Enterprise), Apache Kafka, Solace, and/or TIBCO EMS. Nastel claims this is a differentiator.

Nastel XRay and the Nastel platform can automate corrective and preventive actions via scripting and the use of APIs. Integrations with ticketing systems such as ServiceNow, event management systems, and collaboration tools enable automation wherever it is relevant.

Nastel provides out-of-the-box, configurable dashboards, views, and other visualizations and reporting to meet different business needs. Viewlets, which can have their own URL, provide a summary of the number of objects (such as events, activities, or snapshots) and give operations teams a way to share critical information with other IT groups and with business users. A number of report types are available for performance, analytics and audit, alerts, exceptions, and hotspots, in addition to user-created ad-hoc reports and web-based, iOS, and Android reports.

The Nastel platform monitors end users, systems, and applications, as well as system connectivity.

Strengths: Nastel has outstanding capabilities in automation, dashboards and reports, and data consumption. In addition, the open nature of the tool makes it a good fit for open-source shops looking to leverage AIOps. The ability to customize functions also provides more flexibility. Nastel provides peerless awareness of middleware message flows.

Challenges: The downside of having a more extensible framework is the added complexity and learning curve that Ops teams may find problematic. The tool has a focus on message flows and application flows, so XRay used in concert with other AIOps tools may be a better option for tracking enterprise-wide awareness beyond its initial message and application flow scope. Nastel is weak in its support for OpenTelemetry data, and it does not contribute to the OpenTelemetry project but has stated it plans to do so in 2022.

New Relic

New Relic is a San Francisco-based company founded in 2008. Its observability platform, New Relic One, is targeted at all enterprise verticals including technology, retail, finance, healthcare, media, industrials, and public sector, with a focus on forward-thinking organizations looking for innovative solutions to their IT problems. The company's revenues are increasing rapidly, reaching $753 million by 2021, up from $600 million in 2020.

New Relic One is a cloud-based observability platform that provides APM as well as infrastructure, browser, real user, synthetics, mobile, AIOps, and native client monitoring.

New Relic dashboards include a library of prebuilt charts and templates, which are customizable. Users can also create their own dashboards and reports using New Relic's programmable platform. Data can be visualized via the APM platform, browser, mobile, infrastructure, and synthetics agents, as well as by third-party instrumentation such as Prometheus, DropWizard, Zipkin, OpenTelemetry, and Fluentd. New Relic claims that more than 50 billion events can be analyzed in a single query. Users can use either NRQL to create queries or the guided point-and-click experience with the data explorer. Dashboards as code are also supported using the New Relic Terraform provider, and the NerdGraph API can be used to create, configure, and export dashboards.

New Relic supplies more than 400 integrations through out-of-the-box bundles and exporters, which provide quickstart capabilities to enable enterprises to start monitoring a wide range of third-party products and environments quickly, including .NET, Java, AWS, Azure, and GCP services, Kubernetes and Docker, as well as New Relic add-ons.

New Relic provides native support for OpenTelemetry with a single, fully managed, highly scalable Telemetry Data Platform. New Relic also contributes to the OpenTelemetry project.

The platform provides flexible, dynamic infrastructure observability for applications and services running in the cloud, or dedicated container hosts running in orchestrated environments, including hybrid and multi cloud setups, plus bare metal, virtual machine, and on-host integration support. With infrastructure monitoring, users can connect health and performance data of cloud-based or on-premises hosts to application context, logs, and configuration changes.

Strengths: New Relic is particularly strong in its dashboards and reports, cloud monitoring, and systems integration capabilities. The platform is easy to manage on a daily basis.

Challenges: As a SaaS-only offering, New Relic presents challenges for hybrid enterprises making the journey to the cloud.

OpsRamp

OpsRamp was founded in 2014 to help solve critical pain points for enterprise IT organizations and MSPs. The OpsRamp platform provides monitoring for cloud and on-premises infrastructures and can resolve incidents. OpsRamp's AIOps solution is a service-centric platform comprising intelligent event and incident management, alert correlation, automation, and remediation, and hybrid discovery and monitoring. Support is provided for more than 2,500 integrations. It has a multitenant, multitiered architecture allowing individual clients or customers to be managed as independent tenants. The OpsRamp platform, which features hybrid infrastructure and applications observability, ML, and process automation, is built on a SaaS platform. For customers and partners, this translates into hybrid capabilities that include discovery and monitoring for observability, event and incident management, as well as remediation and automation, all from a single, unified product.

OpsRamp includes an IT process automation and remediation framework to enable the auto-resolution of critical issues or outages, and to run repetitive mundane tasks, via run book automation scripts using the scripting language of choice, such as PowerShell, Python, or shell scripting. It allows standard operating procedures, incident remediations, and day-to-day automation policies to be stored in a single location. A built-in library of commonly used policies that automate and standardize IT infrastructure operations is available. OpsRamp supports ad hoc and scheduled incident resolution as well as runbook automation. Integration with workflow automation engines such as Ansible that trigger workbooks is also supported.

Dashboards and reports are available out-of-the-box, with curated dashboards, standard report templates, customizable dashboards, and reports based on requirements. Also included are alert optimization analytics and the ability to generate inferences for root cause and symptom alert placeholders.

AI is used to create actionable insights in areas such as monitoring for anomaly detection and predictive alerting, and in event management for alert rationalization and probable root cause. The AI/ML feature learns patterns from native and third-party events that are ingested, and it assigns dynamic thresholds based on the behavior of KPIs for both availability and performance metrics, over a period of time. From this information, it is able to predict the most likely cause of an issue.

Out-of-the-box plug-ins and no-code custom integrations based on API and webhooks enable integration with collaboration tools.

OpsRamp can displace some existing tools, but the deployment method allows choices and does not mandate the replacement of all the tools it may impact.

Strengths: The no-code integration process is a plus. OpsRamp has good capabilities across the key criteria of automation, learning systems, dashboards and reports, data consumption, cloud monitoring, and systems integration.

Challenges: OpsRamp is a SaaS-only offering and may be difficult for hybrid enterprises to implement. OpsRamp's support for the use of OpenTelemetry is weak, and it's not a contributor to the OpenTelemetry project.

PagerDuty

PagerDuty was founded in 2009, and is headquartered in San Francisco, California, with offices in Atlanta, Toronto, London, Lisbon, and Sydney. More than 19,000 companies are using PagerDuty, including 60% of the Fortune 100, with more than 1 million users. It focuses on a range of industries, including technology, retail, financial services, healthcare, government and education, and nonprofit.

PagerDuty's AIOps offering comprises incident response and event Intelligence, with the option to integrate with PagerDuty Process Automation (Rundeck) for an end-to-end solution. Customers can purchase Digital Operations, which is the core product, with event and analytics capabilities (or add event Intelligence to their business plan). Additional automation capabilities can be added according to need. Integrations with more than 650 technology partners are available, enabling the solution to connect into any tech stack based on a customer's specific requirements.

Automation is an important area for PagerDuty, and it has adopted an automation-first approach to AIOps. To support this priority, it has made two recent acquisitions:

- Catalytic, a no-code workflow automation platform, supports efficient and digitized operations, and will provide new use cases in finance, human resources, and supply chain workflows.
- Rundeck, which provided DevOps automation for enterprises, adds intelligent machine automation, including auto-remediation and self-healing, to PagerDuty's incident response offering. PagerDuty has put its Automation Actions on-platform, and has created a cloud version of Rundeck called Process Automation. An API is provided to allow access from external applications including SOAR systems, or outbound to cloud or on-premises management systems.

PagerDuty is hosted in AWS with deep integrations across the stack that include Azure ADO and GCP. The AIOps tool can share data and services with other tools, including those for monitoring, configuration management, ITSM, CMDB, security, FinOps, and DevOps. It can also consume runbook data to allow automated troubleshooting or remediation.

PagerDuty supports OpenTelemetry as a user but does not contribute to the project.

PagerDuty was designed to be easy to implement, able to work out-of-the-box via a radio button to turn on capabilities, such as intelligent alert grouping or auto-pausing of notifications for transient alerts. The ML capability de-duplicates, suppresses, and reduces noise.

Strengths: Strengths for PagerDuty include the flexibility, manageability, and ease of implementation of the platform, as well as its minimal tool displacement requirements. It is particularly strong in automation, data consumption, cloud monitoring, and systems integration.

Challenges: PagerDuty has recently expanded into AIOps, and though it has a strong incident and task management offering, the AIOps solution is still proving itself in the market.

ScienceLogic SL1

ScienceLogic is a private company headquartered in Reston, Virginia, with offices in the UK, Taiwan, Singapore, and Australia. Its single platform provides monitoring, business services, and automation. The ScienceLogic SL1 platform includes patented discovery and data collection techniques that provide visibility across the entire IT infrastructure with many legacy and cloud-native components.

ScienceLogic's SL1 platform provides analytics and automated IT capabilities to augment the observability and monitoring of hybrid and multicloud environments. The objective is to unify distributed IT systems, bridging the gap between infrastructure applications and business services to apply analytics that drive IT operations automation. The platform collects all data from cloud and data center environments with its own proprietary data discovery mechanisms, supporting multi cloud and hybrid-cloud environments. It also collects data from other data sources including APM, data exchange module (DEM), and internet of things (IoT). SL1 uses ML-based behavioral correlation and anomaly detection to accelerate root-cause analysis. It auto-correlates events, changes, and anomalies to reduce noise, identify service-impacting issues, and make recommendations for troubleshooting and remediation actions.

ScienceLogic provides prebuilt workflow automations and the ability to create custom workflows with a low/no-code automation and an action policy builder. Out-of-the-box workflow automation PowerPacks are available for incident/notification/collaboration, CMDB/inventory, configuration and change management, DevOps, security, and orchestration. Another resource is a library of best-practice, run-book automations built for troubleshooting and remediating specific technologies, including Cisco, Citrix, F5, Juniper, NetApp, Linux, VMware, MSFT Windows, Hyper-V, and Dell EMC.

Integration with ITSM tools such as ServiceNow, Cherwell, and Atlassian allows the bidirectional synchronization of data to maintain CMDB accuracy in real time. Tickets can be created automatically, with routing, updating, and closing of the tickets also automated. Key stakeholders can be informed and teams can collaborate through PagerDuty, OpsGenie, Microsoft Teams, Slack, xMatters, AWS Incident Manager, and Azure Sentinel. Scheduled maintenance windows can be set up to reduce incident noise. Planned and emergency changes in ServiceNow as well as configuration changes in Restore Point can be correlated with performance events and anomalies to determine root cause and allow for changes to be rolled back through change management, DevOps, and/or orchestration tools.

Data can be imported from physical, virtual, software-defined, and cloud-based network, storage, and compute resources running on-premises or in a multi cloud estate. Users can also build their own monitoring using technologies such as APIs, CLIs, REST, and JMX. There are low-code automated IT and data sync workflows, as well as extended monitoring and syncing capabilities.

ScienceLogic has a large integration catalog comprising more than 500 integrations, available via the PowerPack Library. It provides an SDK for the creation of custom integrations.

A limitation of ScienceLogic is that it does not provide support for OpenTelemetry, either as a user or a contributor.

Strengths: ScienceLogic is particularly strong in automation and data consumption.

Challenges: ScienceLogic does not support the OpenTelemetry initiative either as a user or a contributor. Integration with SecOps systems is a challenge.

ServiceNow AIOps

ServiceNow was founded in 2004 by Fred Luddy, with the vision of a cloud-based platform that would allow users to route work effectively through the enterprise, using workflows. Headquartered in Santa Clara, California, the ServiceNow platform incorporates comprehensive AIOps capabilities, thanks to its acquisition of Israel-based Loom Systems, which extended its existing AIOps capabilities. ServiceNow acquired Lightstep over a year ago. Lightstep is a founding contributor (co-founder) to OpenTelemetry. ServiceNow provides IT with control over both on-premises and cloud-based resources. ServiceNow is differentiated from other vendors by its Now Platform that performs a variety of functions, of which AIOps is just one.

ServiceNow AIOps provides tab-based alert clustering without a complete CMDB, automated temporal analysis to validate the ML on a regular basis, topological analysis to obtain basic discovery or service mapping, and AI analysis of logs for anomalies in real-time.

Dashboards allow visualization of prediction trends and their impact on the business, providing views on the reduction in resolution times, its impact on the number of issues resolved, monthly prediction coverage, and accuracy trends. ServiceNow is known for its extensive dashboards. The ease of creating dashboards has improved, but still remains challenging until sufficient learning has taken place.

ServiceNow provides connectors to third-party products such as Dynatrace and New Relic, to import application data. Service Graph Connectors import third-party data into ServiceNow Service Graph. They are built by ServiceNow and its technology partners. This is an evolution of the ServiceNow CMDB, extending coverage to planning, application development, deployment, performance, cost, and business processes, as well as other areas, by implementing the ServiceNow Common Service Data Model (CSDM).

A full AIOps implementation from ServiceNow can displace all existing tools; however, the ServiceNow platform provides compelling reasons to consider ServiceNow as a single vendor. The cost in both time and money may make the entire ServiceNow platform, along with the AIOps solution, difficult to integrate in a large enterprise.

ServiceNow is a SaaS-only deployment and integrates with onsite systems. A customer-managed implementation of ServiceNow does exist; however, no new deployments are planned, and existing deployments are moving to the SaaS platform.

Strengths: ServiceNow presents a total package of ITOM solutions along with its AIOps offering. It can be a one-stop shop for all ITOM and other IT systems. Areas where ServiceNow has outstanding capabilities include automation, learning systems, dashboards and reports, and systems integration.

Challenges: The UI for ServiceNow can be challenging, though this is mitigated to some extent by an excellent training and certification system. The full tool displacement required for the AIOps solution from ServiceNow will present strategic and tactical challenges for some shops.

Splunk

Splunk has been in the IT monitoring business for more than 15 years. In 2019, it acquired SignalFx (founded in 2013) and Omnition (founded in 2018), which enhanced the usability of the Splunk platform and transformed it into a full observability platform.

The Splunk solution combines monitoring, troubleshooting, and incident response solutions that boost application modernization initiatives. Splunk is an integrated, full-stack, multi cloud enterprise solution that comprises Splunk Observability Cloud and Splunk Enterprise and brings together a number of monitoring features—infrastructure, application performance, digital experience, real user, synthetics, log investigation, AIOps, and incident response—into a single platform for any hybrid-cloud application environment. It provides full coverage from on-premises to hybrid- and multi cloud environments.

Splunk incorporates a number of automated features, including the ability to send episodes and alerts into Splunk SOAR and use its capabilities for IT orchestration, automation, and remediation. There are more than 350 supported playbooks for SOAR on Splunkbase, and users can also create their own. There are bidirectional integrations with popular ITSM platforms such as ServiceNow, BMC, and Jira, and automated ticketing is available to improve incident response and operator workflow between these platforms.

Splunk Observability ingests, analyzes, and stores all transactions from all systems. Splunk encourages enterprises to send all their metrics, traces, end-user spans, and log data without sampling or filtering, and to retain it for a reasonable period of time.

Splunk's ML capabilities are applied throughout the platform. They offer predictive alerting that enables users to receive alerts about system degradation before it occurs, using ML and historical data to predict the future health of a service.

Adaptive thresholds for alerts can be enabled based on the statistical distribution of historical data. ML algorithms automatically update thresholds based on observed behavior, making recalculations nightly to ensure that changes in behavior do not trigger false alerts. ML is also used to trigger alerts for exceptions and deviations.

Prepackaged ML models are provided for Splunk data, KPIs, and service model summarized data in order to reduce mean time to repair (MTTR). ML concepts such as out-of-the-box queries, custom visualizations, and guided assistants are available to allow users to build their own models. ML is also used for noise reduction, which allows events from Splunk tools and third-party data sources to be grouped based on their similarities. Preconfigured executive dashboards for organization leaders that present business KPIs and business context are also available, and include metrics for service availability status, number of contracts being processed, and how much revenue certain services are generating. Additional out-of-the-box monitoring capabilities for various technologies and subject matter expert (SME) roles are also available, including entity types, KPIs, services, service templates, correlation searches, dashboards, service health analyzers, and glass tables.

Splunk displaces many existing monitoring tools. The advantages of using a single vendor for monitoring and AIOps are many; however, embracing the entire Splunk platform will require strategic planning and perhaps professional services. Tools within the AIOps suite can be deployed individually.

Strengths: Splunk is strong in automation, AI/ML learning systems, dashboards and reports, data consumption, and cloud monitoring. Splunk Observability relies exclusively on OpenTelemetry to capture metric, logs, and trace data from customers' environments, and the vendor is also a co-founder of and an active contributor to the project. Splunk has many deployment options, including SaaS and onsite.

Challenges: A full Splunk deployment may require professional services. Splunk provides bidirectional integrations with ServiceNow, Cherwell, and BMC Remedy/Helix, but not Manage Engine. Splunk does not currently support change detection or federated, distributed, edge AI/ML. Although it offers auto-remediation and automation capabilities, Splunk is actively working on enhancing them to provide full autonomous intelligent remediation functionality that can resolve incidents with minimal user intervention.

Sumo Logic Continuous Intelligence Platform

Sumo Logic is a SaaS-based, cloud-native, multitenant observability platform. It was built originally as a log management, big data analytics, and SIEM solution, but the company has added tracing and metrics to evolve the product into a full observability platform. Sumo Logic's main target is the enterprise market, but it is also suited to the SMB market.

Sumo Logic's Continuous Intelligence Platform ingests and analyzes data from applications, infrastructure, security, and IoT sources. It then develops unified, real-time analytics. The platform employs AI/ML to create a smooth user experience when exploring logs, metrics, and traces.

This is a cloud-native, multitenant platform that provides more than 175 integrations to sources from which data can be collected and aggregated. Customizable dashboards allow logs, metrics, and performance data to be monitored and visualized across the full stack. Real-time analytics enable potential cyberattacks to be identified and resolved to prevent breaches, and ML algorithms send alerts when issues are identified.

One of the strengths of the platform is its cloud monitoring capabilities. Data can be ingested and analyzed from multiple clouds, including AWS, Azure, GCP, and private clouds. A variety of methods are used for ingesting and analyzing data, including host (installed) collectors, cloud-to-cloud collection, and HTTP endpoints (push based). Sumo Logic is agnostic as to the origin or location of data, which can be collected via streams and API-based methods. The solution is fully integrated with AWS CloudWatch, GCP Stackdriver (Operations Suite), and Azure Monitor for bringing in data.

The platform also has good integration capabilities. An example of a unidirectional integration between ITSM and event and incident management is enabled through ITOM webhook integrations that allow Sumo Logic to open a ServiceNow incident or event in response to an alert. Sumo alert status ensures that incidents are kept up to date. ServiceNow incidents (with context) can also be created manually from Sumo Logic. Integration with Service Graph allows users to autodetect and update ephemeral AWS and VMware data to the ServiceNow CMDB in real time.

Data consumption is also an area of strength for Sumo Logic, with a number of methods available. There are installed collectors for logs and metrics from on-premises applications and infrastructures; hosted collectors and cloud-to-cloud collectors for data from cloud infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS services; and a Kubernetes collection framework that embeds Prometheus, fluentd, and fluetbit to support logs, metrics, and events collections from Kubernetes. In addition, an OpenTelemetry collection framework supports metrics and trace collections; and AWS Cloudwatch, Kinesis, and X-ray collectors are available for AWS infrastructure.

Sumo Logic natively supports OpenTelemetry data collection as a primary data source, with more than 50 metric sources and cloud sources, while Splunk and SignalFx and traces (Jaeger, Zipkin) are supported. Sumo Logic contributes heavily to OpenTelemetry as an individual via its CTO.

Strengths: Areas of strength for Sumo Logic are data consumption, cloud monitoring with support for multiple clouds, systems integration with more than 175 integrations, and support for OpenTelemetry utilization.

Challenges: Sumo Logic lacks support for change detection, which is an important emerging technology.

Zenoss

Zenossis is headquartered in Austin, Texas, with an office in the UK; it was co-founded and incorporated in November 2005. Zenoss Cloud provides AIOps with full-stack monitoring; it is an SaaS-based intelligent IT operations management platform that streams and normalizes all machine data to prevent service disruptions. Zenoss monitors 1 million resources globally and more than 70 billion data points a day, with more than 200 million daily data points per customer. The company targets organizations in the federal, financial services, healthcare, service provider, and technology sectors. For federal clients, it is deployed on GCP, which is fully FedRAMP certified. Zenoss does not require the displacement of existing tools.

Zenoss monitors GCP, AWS, and Azure, as well as other cloud resources including multicloud environments and on-premises environments. All public cloud entities are covered, including regions, instances, and subnets, with visualizations of how failures in individual cloud components impact application performance. Private cloud monitoring includes OpenStack, Apache CloudStack, VMware, and vCloud Director.

One of the strengths of Zenoss is its learning systems. It produces real-time dynamic models of end-to-end IT services and applications, allowing users to visualize and understand all dependencies. Supervised ML provides dynamic visibility of key events. Root cause analysis is identified through real-time modeling, which provides awareness of end-to-end infrastructure-related risks, and predictive analytics is enabled.

Zenoss collects real-time metrics, and a wide variety of data—dependency, streaming, event, log, agent, application, and network performance. ZenPacks allow configuration information to be collected from third-party systems using standard APIs and protocols, including SNMP, WinRM, and SSH. ZenPacks are available for Google Cloud, ServiceNow, Nutanix, and PagerDuty. Four categories of ZenPacks are available: commercial, open source, community, and subscription. Zenoss creates many of the ZenPacks, some of which are released freely into the community, while others are available via a paid subscription or service agreement. Additional ZenPacks are created and supported by community members.

Zenoss displaces a minimum number of tools. Tactical and strategic planning can allow Zenoss to monitor in areas where limited monitoring exists.

Strengths: Areas of strength for Zenoss are learning systems, data consumption, and cloud monitoring. Also, it does not displace existing tools.

Challenges: Zenoss does not directly support OpenTelemetry; however, a custom ZenPack with ZenLib pythonSDK can be created. It does not contribute to the OpenTelemetry project.

6. Analyst's Take

There are some significant differences among AIOps solutions, and as the number of solutions continues to grow, choosing the right vendor has become more complicated. Early leaders in this space didn't displace many existing tools or technologies, but that's changing. The number and type of tools replaced by AIOps solutions is a defining feature in today's AIOps space.

Total platform solutions that displace all existing tooling have powerful capabilities, but at the cost of change and all the disruption that it brings. IT has always been resistant to change, especially in large enterprises where AIOps solutions are likely a good fit. BMC, ServiceNow, IBM, Broadcom, Micro Focus, and the new platform vendor Splunk provide robust AIOps solutions. For enterprises already invested in these solutions, the choice is obvious. For decision-makers looking into these platforms for the first time, the process is more complicated. Each of the vendors provides a piece-by-piece solution, with the goal of becoming a one-stop solution for all monitoring and AIOps. Therefore, identification of a longer-term strategy is essential during the selection process.

Another category of AIOps solutions displace fewer incumbent tools. Many of these solutions derive from specific monitoring aspects of ITOM and, via acquisition or in-house development, are now marketing themselves as AIOps solutions. Dynatrace, New Relic, and Cisco (AppDynamics) come from the APM world. DataDog came from infrastructure monitoring. PagerDuty's heritage is that of incident task management and scheduling, and it has expanded into the AIOps world. Splunk began as a log management solution and was once considered part of this category; however, it is now more of a platform player and so is not included in this group.

Also included in this category are ScienceLogic, OpsRamp, Interlink, and SumoLogic. These solutions cause less tool displacement but do not come from APM or log management backgrounds.

Dynatrace is a strong player in the Maturity/Platform Play quadrant of the Radar; however, its network device monitoring is limited to SNMP traps, which restricts its overall usability in large organizations. SNMP management is often daunting when large numbers of devices from different vendors must be managed. There is no support for Netflow or probe-based network device monitoring.

These solutions are probably a better fit for enterprises that aren't as strong in the vendor's core strength area but are robust in other areas. The data ingestion and integration strengths vary, but the solutions are competent AIOps remedies.

Vendors such as Moogsoft, BigPanda, and, to a lesser extent, Zenoss, are pure AIOps solutions with no domain-specific characteristics. No existing tools are displaced; however, additional work may be necessary to complete data ingestion and integration. Some vendors in this category— Elastic, and Logz.io—are open source and may fit enterprises primarily using open-source platforms.

Moogsoft can consume data from essentially any source and makes the process easier over time. The bidirectional integration with existing tools can be challenging but is continually improving. The company's recent pivot to a SaaS solution lacking full parity with the onsite solution requires enterprises to look carefully at this sector-leading solution.

This report identifies four vendors as Innovation players—Centerity, CloudFabrix, Digitate, and Nastel. Each provides a complete AIOps solution with unique capabilities.

Centerity offers innovative technologies for edge devices, including POS systems, servers, ATMs, security cameras, and temperature-controlled devices. It also offers innovative technologies for radio systems and infrastructure (transmission equipment, microwave systems, log recorders, and IOT devices) for public safety and professional communications. If the enterprise needs AIOps in a diverse technology environment, including one with edge devices, Centerity may be a unique fit.

CloudFabrix, with its Robotic Data Automation Fabric, provides a distributed AIOps model that's unique. It uses a supervised training model, so the need to train models and the poor ease of use with the UI may make this vendor a more challenging choice for some enterprises. However, the UI is constantly improving, and the data fabric and OpenTelemetry give the solution data collection capabilities beyond most AIOps offerings, while the unsupervised training of data models has improved.

Digitate is innovative in automation. Enterprises looking to automate their environment to the greatest extent possible may want to investigate its AIOps solution, which extends automation to more settings than most others

Messaging and message queues (and streaming) have unique requirements within IT operations management monitoring. Many AIOps solutions can monitor the messaging endpoints, but Nastel also offers monitoring and intelligence to message services themselves such as IBM MQ, Kafka, and others. The company's leading-edge technologies shine in the transaction-heavy industries of banking and financial services. Nastel provides its own AIOps solution but may also be used to augment another AIOps deployment where messaging is of primary importance.

In the area of emerging technologies, the investigation into whether the edge of the enterprise can be modeled independently brought the realization that IoT and other edge technologies may require some consideration. A few vendors have explored AIOps for the edge, but only Centerity, CloudFabrix, and Sumo Logic, have made strides. At some point, sending all data to a single AI/ML component will break down because of computing, memory, storage, or other issues. Vendors with designs that allow distributed AI/ML may be better positioned when the AIOps market reaches that point.

Another needed functionality that is often acknowledged but rarely dealt with is shadow change detection. Shadow changes are unauthorized changes that appear within the enterprise, typically from an unknown source, such as ITSM or DevOps, but are not usually detected as an anomaly. Moving an Ethernet cable on a data center switch is an example. AI/ML systems that can detect shadow changes and notify about them may have an advantage in future iterations of AIOps.

This year's crop of AIOps solutions provides enterprises with more choice than ever. Capabilities have increased across the board, and vendors may have unintentionally differentiated themselves more so with respect to the tools they displace than by any of their new features. Enterprises looking to deploy an AIOps solution should examine its capabilities, its impact on existing tools, and the longer-term strategies needed to achieve operational awareness in their organization.

7. About Ron Williams

Ron Williams

Ron Williams is an astute technology leader with more than 30 years' experience providing innovative solutions for high-growth organizations. He is a highly analytical and accomplished professional who has directed the design and implementation of solutions across diverse sectors. Ron has a proven history of excellence propelling organizational success by establishing and executing strategic initiatives that optimize performance. He has demonstrated expertise in planning and implementing solutions for enterprises and business applications, developing key architectural components, performing risk analysis, and leading all phases of projects from initialization to completion. He has been recognized for promoting effective governance and positive change that improved operational efficiency, revenues, and cost savings. As an elite communicator and design architect, Ron has transformed strategic ideas into reality through close coordination with engineering teams, stakeholders, and C-level executives.

Ron has worked for the US Department of Defense (Star Wars initiative), NASA, Mary Kay Cosmetics, Texas Instruments, Sprint, TopGolf, and American Airlines, and participated in international consulting in Qatar, Brazil, and the U.K. He has led remote software and infrastructure teams in India, China, and Ghana.

Ron is a pioneer in enterprise architecture who improved response and resolution of enterprise-wide problems by deploying "smart" tools and platforms. In his current role as an analyst, Ron provides innovative technology and strategy solutions in both enterprise and SMB settings. He is currently using his expertise to analyze the IT processes of the future with particular interest in how machine learning and artificial intelligence can improve IT operations.

8. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

9. Copyright

Data Infrastructure, AI & Analytics