GIGAOM



Image credit: Tuadesk

David S. Linthicum, Ron Williams, Michael Delzer
Sep 3, 2021

GigaOm Radar for AIOps Solutions v2.0

Assessing Cutting-Edge Tools for Managing the Rising Complexity of Enterprise Operations

Cloud & Infrastructure

GigaOm Radar for AIOps Solutions

Assessing Cutting-Edge Tools for Managing the Rising Complexity of Enterprise Operations

Table of Contents

1 Summary

2 Market Categories and Deployment Types

3 Key Criteria Comparison

4 GigaOm Radar

5 Vendor Insights

6 Analyst's Take

7 About David Linthicum

8 About Ron Williams

9 About Michael Delzer

10 About GigaOm

11 Copyright

1. Summary

The importance of AIOps has increased in response to the rapid adoption of cloud and edge computing and the rising complexity these environments create. Intelligent tools act as a force multiplier for ops teams, helping them adapt to escalating demand even in the absence of budget and staff increases. AIOps also helps address the operational challenges of having cloud-based applications and data that must continue to operate with existing systems, such as mainframes, x86 clusters still crowding data centers, and increasingly complicated networks.

AIOps tools are growing in several directions. Most vendors in the traditional operations tools space have incorporated an AI engine and rebranded their tool with AIOps. Additionally, there is a cohort of startups that have developed purpose-built AIOps tools.

The development of hybrid AIOps tools follows the normalization of the market, leading to vendors combining technologies. Some vendors are buying their way into the AIOps space via acquisitions. In this scenario, vendors integrate traditional operational tools with AI technology, while new upstarts address a niche or add new features to the AIOps landscape. Finally, there are also larger cloud providers dipping their toes into the market. These providers are building tools that manage their native services and cross-cloud tools that manage multiple cloud platforms.

All these tools are data-oriented. They gather data from as many sources as possible, using their connectors and integration or even leveraging other instrumentation to connect with systems. Combining software has confused the AIOps market, as some tools focus only on data analysis and not how it's collected. Others focus on collection and analysis but may not support complete awareness of the state of the enterprise

If that's not confusing enough, we've also found AIOps tools take different approaches to how AIOps works. Approaches to the remediation of issues, integration with other cloud systems, security, governance, and even cost accountability make vendor selection more complex. The confusion multiplies when the term "AI" is used to describe a rules-based heuristic system with human supervision.

In contrast, others have a core AI module with true neural capabilities. This difference can determine whether a system can ingest a new data set with minimal human intervention or if it requires substantial effort to add new data to the system.

As we close in on the measure of a good AIOps tool, the "it depends" factor becomes important to understand. The complexity of the answer depends on the types of systems you're looking to monitor and observe, the data storage in place, expectations (including supporting a customer experience), applications employed, and other operational systems such as security and governance. Thus, it's less about selecting the best AIOps tool, and more about selecting a tool or tools that will meet your overall cloud and non-cloud operational needs in the near- and long-term.

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

AIOps tools support several varied deployment models and multiple target market segments, as shown in **Table 1.** This report considers two market segments: large enterprises and medium-to-small enterprises. We also consider three deployment models for the AI engine hosting:

- **SaaS AI**: These vendors offer only an AI engine running in a SaaS platform. These Saas solutions use AIOps tools for public clouds, including hybrid and multi-cloud, that may or may not include a private cloud.
- **On-premises AI**: The AI for the tool runs on systems traditionally found on-premises. These are often traditional enterprise monitoring tools, now recast as an AIOps tool or tools that focus on systems typically found within a data center. The software may be able to run in VMs or containers that a customer hosts with their environment in a public cloud provider. In this category, the customer runs the software where they want, but owns all operational responsibilities.
- **Holistic:** In this approach customers can choose the location of the AI engine without impacting system functionality. Data ingestion is from the cloud and on-premises sources.

Table 1. Vendor Positioning

	MARKET SEGMENT		DEPLOYMENT MODELS		
	Large Enterprise	Medium to Small Enterprise	SaaS	On-Premises	Holistic
BigPanda	+++	++	++	–	–
BMC AIOps	+++	++	++	++	++
Broadcom	+++	++	++	++	–
Centerity	++	++	++	++	++
Cisco AppDynamics	+++	+	++	++	++
CloudFabrix	+++	++	++	++	++
Datadog	++	++	++	–	–
Dynatrace	+++	+++	++	++	++
IBM	+++	++	–	++	–
Micro Focus	+++	++	++	++	++
Moogsoft	+++	++	+	++	++
Nastel	++	+	++	++	++
New Relic	+++	+++	++	–	–
OpsRamp	++	++	++	–	–
Splunk	+++	+++	++	++	++

+++ 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 2021

3. Key Criteria Comparison

As covered in the AIOps Key Criteria Report, this report evaluates AIOps tools based on their core functionality, including the following table stakes:

- **Observe:** The gathering of data from any number of systems to find patterns for analysis and action.
- **Correlate**: Grouping massive amounts of system data (noise) in meaningful ways. This includes determining patterns.
- **Analyze:** Determining problems and their root cause.
- **Collaborate:** Presenting observability findings to ops team users, and enable automated processes that can respond without human intervention to resolve issues.
- **Respond:** Taking action in response to problems and launching an automated fix or collaboration to achieve a resolution.
- **Inform**: Providing reporting and dashboarding so AIOps users can see both strategic and tactical data.
- **Use AI:** Driving value within all of the above functions by leveraging the capabilities of AI.

The above criteria diverge from the categorizations used last year in our report, which focused on the general behavior of the tools and not the supported features. As AIOps has evolved, this list of categories will be more helpful in making a tool selection.

Figure 1 (from the Key Criteria Report), helps you understand which categories are most important and which should be weighted to reflect your specific needs. Seek a specific mix of features and functions that are best for your enterprise when selecting AIOps tools. **Figure 1** is just an example, using sample data.

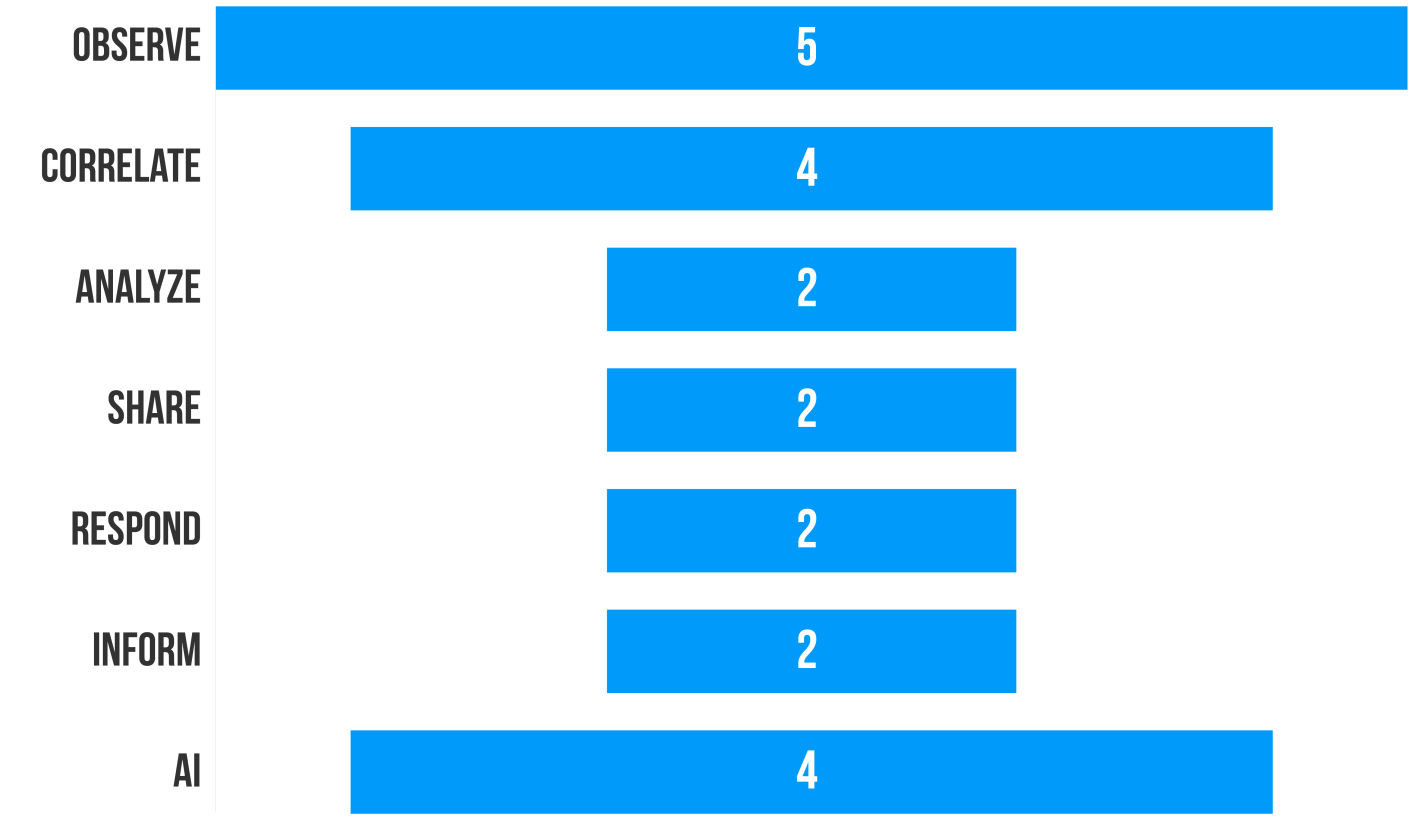


Figure 1. Example of the Mix of Capabilities an AIOps Tool Might Present

Building on the findings from the GigaOm report, "Key Criteria for Evaluating AIOps," **Table 2** summarizes how each vendor included in this research performs in the areas we consider differentiating and critical in this sector. The objective is to provide a snapshot of the technical capabilities of different solutions and define the perimeter of the market landscape. **Table 3** shows scoring around evaluation metrics, which provide insight into the broad value an AIOps platform can have to an organization.

Key Criteria

Automation: The ability to onboard new applications and create useful analysis with minimal human intervention, with the extensibility to automate remediation for well-known processes. This criterion includes the following considerations:

- **Proactive/self-healing operations:** The AIOps tool is able to solve problems automatically without human intervention, either through external or internal orchestration tooling, or leveraging an automated ticketing system.
- **Automation (API):** The tool provides an API allowing access from external applications that need

to include capabilities for inbound from security SOAR systems or outbound to cloud or on-premises management systems.

- **ITSM and CMDB updates:** Workflows can update ITSM and CMDB upon changes.

Learning systems: The AI engine is able to learn from the data being consumed by the AIOps tools and change behavior as it's exposed to more training data. Some tools are rules-based, whereas the true AI/ML systems are not. They may have some values that must be set, or information about what can be correlated, but the core engine is AI.

Dashboards and reports: Dashboards are customizable, as is other reporting. Dashboards should be either shareable or exportable so users can have the same experience if that is what management expects. This is typically true for follow-the-sun models or multiple shifts of workers.

Data consumption: The AIOps tool should consume inputs and correlate causation. It should be allowed either to make a change or notify humans, and should grant a unique event channel in tools where the event can be managed. It includes:

- **End-user monitoring:** The tool is able to monitor and manage the end user experience. End-user monitoring, or real-user monitoring, is typically an APM requirement and not something the AIOps tool does by itself. AIOps should consume and use the end user data regardless of the source.
- **System monitoring:** Addresses hardware, OS, storage, and network system data feeds. Includes the ability to consume SNMP, network device flow like Cisco's Netflow, and new feeds like WMI or outputs of OEM management tools like those from HP and Dell.
- **Application monitoring:** While the AIOps tool can see infrastructure resources, there is also visibility directly into applications. Moreover, this visibility needs to include front-end and back-end dependencies like database and application load balancing. IT may also need to include API gateways and service mesh or caching technologies.
- **System connectivity:** This addresses the ability to connect to a wide variety of systems, such as storage, compute, applications, and networks, ensuring those connections are maintained.

Cross-cloud monitoring: The ability to monitor across cloud providers using similar operational features and functions. The tool should also be able to consume feeds or pull cloud vendor APIs to get near-real-time metrics. Ideally, the tool would be able to correlate metrics from one cloud vendor to the corresponding metric from a different vendor.

Integration: The AIOps tool is able to share data and services with other tools such as security and monitoring, including:

- **Cost and usage monitoring:** The ability to monitor usage, cost information, and analytical systems found in other cost governance or traditional enterprise accounting. Support for audit compliance

features enables posting directly to enterprise accounting systems, such as SAP or Oracle Financials.

- **Leveraging agents:** The ability to consume feeds from major vendors' agents, like Oracle OEM or AIOps tool agents, that require their own agents on endpoint devices.
- **Configuration management**: Addresses the ability to let the user see the current infrastructure state, such as by a CMDB.
- **IT service management:** This lets users see change requests and view or create incidents tickets.

DevOps integration: The AIOps tool can see the dev tool chain, including integration with traditional DevOps tooling. This includes the ability to see the outcomes of the continuous deployment process of a DevOps tool chain and correlate that with ITSM change requests validated by the CMDB. So it is always monitoring what is, and not what was.

Table 2. Key Criteria Comparison

	KEY CRITERIA						
	Automation	Learning Systems	Dashboards and Reports	Data Consumption	Cross-Cloud Monitoring	Ops Systems Integration	DevOps Integration
BigPanda	++	++	+++	+++	++	+++	++
BMC AIOps	+++	++	++	+++	+	+++	++
Broadcom	++	++	++	+++	++	+++	+++
Centerity	++	+	++	++	++	+	++
Cisco AppDynamics	+++	++	+++	+++	++	+++	++
CloudFabrix	++	+++	+++	+++	++	++	++
Datadog	++	++	++	+++	++	+++	++
Dynatrace	++	++	+++	++	+++	+++	++
IBM	++	+++	++	++	+	+++	++
Micro Focus	+++	++	++	+++	++	+++	++
Moogsoft	++	+++	+++	+++	++	+++	++
Nastel	++	++	++	+	++	+	++
New Relic	++	++	++	+++	++	+++	++
OpsRamp	++	++	++	++	++	++	++
Splunk	+++	++	++	+++	++	+++	++

+++ 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 2021

Evaluation Metrics Comparison

Flexibility: Refers to the number and types of systems supported out-of-the-box. This includes the type of data gathered, meaning we can see most of the data needed to determine operational

behaviors, both past and present, as well as the supporting predictive analytics. This is the context in which you will consider standards such as OpenTelemetry, but considering all emerging standards is helpful as well.

Manageability: How operations are approached from the unmodified tool. This should include most operational patterns and best practices. Includes BC/DR—the vendor should have an approved disaster recovery plan, so if the primary instance fails, the business is not blind pending restoration of the AIOps system.

Ease of implementation: How easy is it to deploy the AIOps tool and connect with all systems to be monitored? Includes learning approaches—since we are leveraging a native AI system as part of AIOps, we must also understand how the AIOps tool learns over time and the processes to do so.

Usability (use of dashboards and other analytics): The default information externalization approaches make sense and are easy for the ops team to leverage.

ROI/TCO: ROI/TCO was removed from scoring as there was no uniform method to compare all of the vendors.

Table 3. Evaluation Metrics Comparison

	EVALUATION METRICS			
	Flexibility	Manageability	Ease of Implementation	Usability
Big Panda	+++	+++	+++	++
BMC AIOps	+++	++	++	+++
Broadcom	+++	+++	++	++
Centerity	++	+	++	++
Cisco AppDynamics	+++	++	++	++
CloudFabrix	++	++	++	++
Datadog	+++	+++	++	++
Dynatrace	+++	+++	++	+++
IBM	++	++	++	++
Micro Focus	+++	+++	++	++
Moogsoft	+++	+++	++	+++
Nastel	++	+	+	++
New Relic	+++	+	++	++
OpsRamp	++	+	++	++
Splunk	+++	+++	++	++

+++ 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 2021

By combining the information in the tables above, you can gain a clear understanding of the available technical solutions in the AIOps sector.

4. GigaOm Radar

This report synthesizes analysis of key criteria and examines their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 2**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

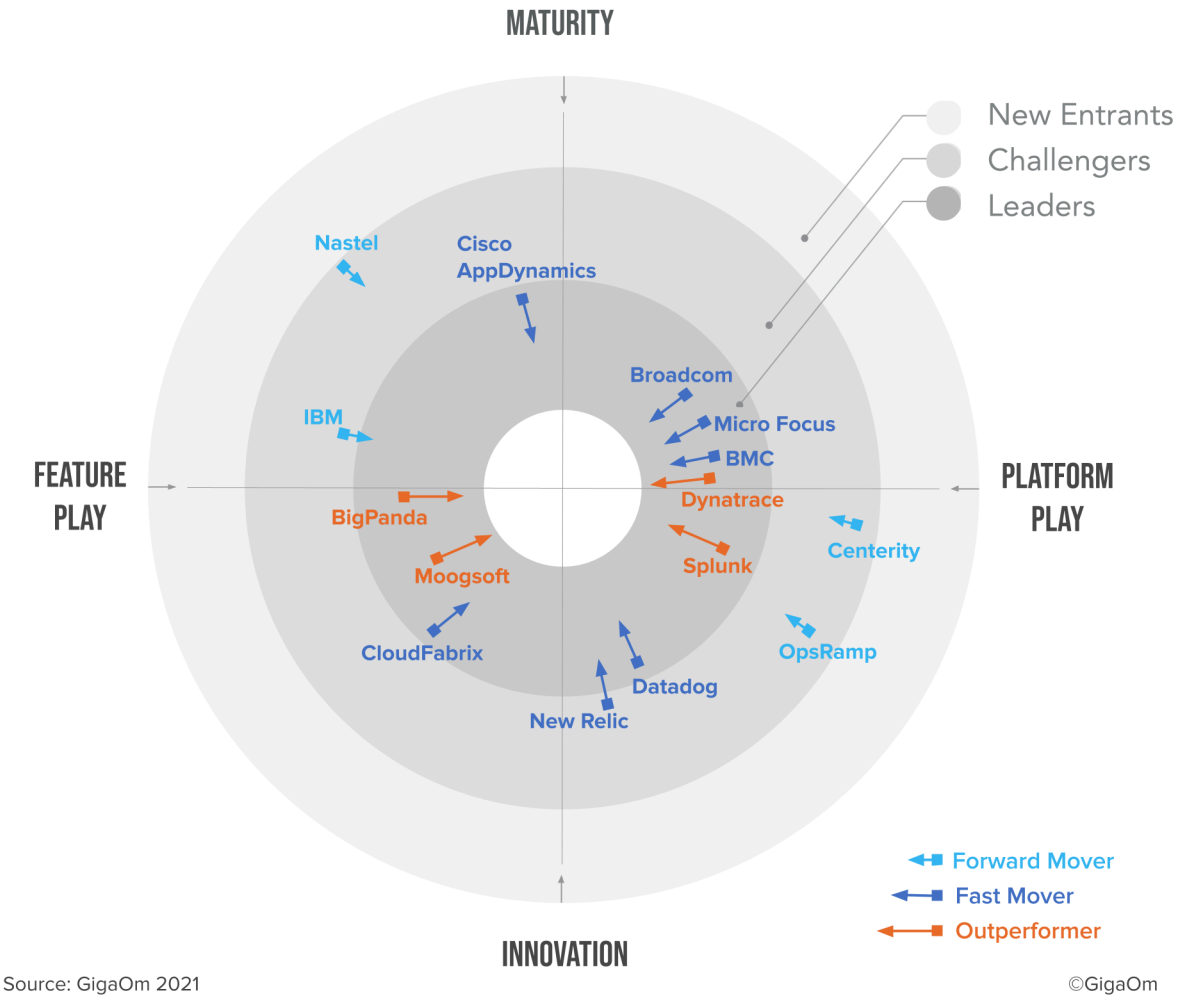


Figure 2. GigaOm Radar for AIOps

The GigaOm Radar **(Figure 2)** plots vendor solutions across a series of concentric rings, with those set closer to center indicating higher overall value. The chart characterizes each vendor on two axes—Maturity versus Innovation and Feature Play versus Platform Play. An arrow projects each solution's evolution over the coming 12 to 18 months. Based on our analysis, we draw the following conclusions:

- **The AIOps space is still evolving:** There are many differences from last year's report in terms of how vendors are assessed and scored. The evolution of this industry is likely to accelerate in

2022, considering the importance of the problems it's solving and the challenges posed in solving those problems.

- **Most vendors increased the number and types of systems supported:** Most also improved their ability to leverage data gathered in more meaningful ways to support observability, including making sense of massive amounts of data using aggregation and correlation to determine patterns to which ops teams can react.
- **Automation is the new normal:** In our last report, some tools lacked support for orchestration, either on their own or through third-party technology. A year later, most AIOps tools actively support native orchestration, third-party orchestration, or both. This helps automate operations such as self-healing or other proactive and reactive actions.
- **AI is leveraged in very different ways:** While some AIOps providers systematically leverage AI, others use it as a loosely coupled service to support analytics.
- **Integration is key to success:** AIOps tools don't do it all. They need to connect to other systems to augment such functions as security operations, governance operations, specialized performance monitoring, and connecting to monitored systems. Many of these tools are therefore best leveraged as an AIOps stack, instead of a single-tool solution. This may result in larger AIOps players purchasing complementary tool providers.
- **There is value in having known brands:** AIOps brands that have been on the market the longest will typically have access to the traditional systems market, using those systems as a jumping off point to include cloud platforms. It's more difficult for lesser-known brands to sell holistic AIOps tools outside of platforms such as cloud, edge, and IoT.

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

One way to summarize BigPanda would be openness. The solution is platform-, vendor-, and technology-domain agnostic and leverages its own integration module called Open Integration Hub. That means it supports and integrates with most of what's already operating in your infrastructure via native and open APIs, and can work with on-premises and/or cloud-based systems.

BigPanda leverages Open Box Machine Learning, its implementation of explainable AI, to help it correlate large amounts of IT Ops data into meaningful information. Another unique feature is the ability to integrate with all your other monitoring and observability tools using BigPanda to create a single-pane-of-glass view. You could consider this AIOps for AIOps.

Using BigPanda's Open Integration Hub to ingest data from a range of monitoring, observability, change, and topology tools positions BigPanda as the highest level of abstraction for driving AIOps. BigPanda applies Open Box Machine Learning to massively reduce the noise, and then correlate and transform that data into actionable incidents. There is also a root cause analysis engine to help operations teams identify environmental changes or the infrastructure and application issues causing an incident.

Other features include integration with different collaboration tools, automated ticket creation, automated notifications, and automatically creating war rooms with the right teams. Automatic bidirectional syncing ensures teams on either side always have access to incident information and updates. Integrations with third-party automation tools also help enterprises drive custom workflow automations such as validation, diagnostics, and remediation.

Strengths: The ability to integrate other operations tools and support both IT Ops and DevOps are key positive differentiators for this tool. BigPanda is essentially "AIOps for AIOps," or the master control center for most operations, as it supports most systems whether on-premises or in the cloud.

Challenges: Custom integrations can be challenging and setting up the tools requires some previous knowledge of the problems and metrics that indicate the problems.

BMC AIOps

BMC AIOps is targeted at mid-sized and large organizations and supports both traditional systems on-premises and cloud-based systems. This heterogeneous support using a single set of tooling and interfaces helps existing BMC customers leverage their existing investments and moves new BMC customers to their AIOps platform.

BMC AIOps currently is seeing a shift from on-premises to cloud deployments. This is due to the many

advantages offered by SaaS, especially lower cost of ownership.

The BMC AIOps feature set includes the ability to leverage four types of operational data, including metrics, events, logs, and topology. The tool can consume data from many third-party data sources as well, and supports most on-premises and cloud-based systems. Mainframe support gives BMC the advantage of serving companies that still have legacy systems in place, which is of course most of the Global 2000.

The BMC architecture supports microservices and container-based architectures, enabling it to support customers' modern applications. The solution uses purpose-built data stores optimized for large-scale persistence of event, metric, and topology data. These data stores are based on Elasticsearch and VictoriaMetrics and provide the ability to scale to meet customer needs. It also provides automation that enables BMC to leverage analytics to detect problems and self-heal.

BMC can manage relationships between components and additional levels of data analytics. It also provides the basic aspects of AIOps including monitoring and anomaly detection. It supports both univariate and multivariate detection.

Finally, BMC supports probable-cause analysis (root cause), using a single-click drill-down to reveal the root cause of a problem in the environment.

The solution operates as a manager-of-managers by incorporating data from a wide range of technologies to provide intelligence, analytics, and automation to deliver service and operations management excellence in a single platform.

Strengths: Leading the other AIOps tools that support legacy systems, BMC spans the management domains from legacy to cloud to provide a core advantage sought by many enterprises. The company's maturity means there will be more resources focused on AIOps and the likelihood of increasing its value moving forward.

Challenges: The legacy heritage may make this tool seem to buyers to be less focused on cloud-based systems. This perception has been improved upon since our last examination, but it remains a consideration. Third-party systems may have difficulty mining BMC's datastores which may be an issue for security groups that need the same content.

Broadcom DX Operational Intelligence

Much like other AIOps stacks from "traditional" providers, AIOps from Broadcom is clearly an existing infrastructure monitoring platform with AI capabilities and a new reach into the clouds. Broadcom is adopting a hybrid cloud strategy, in which traditional systems work well together. While somewhat hindered by Broadcom's "legacy" reputation, the AIOps tool is well-built and up to date.

DX Operational Intelligence is more aligned with organizations that have a mix of legacy and modern

systems; on-premises as well as public cloud-based systems. The solution can correlate monitoring and management data with a focus on applications, infrastructure, and networks. It works with an automation platform to facilitate autonomous remediation. It's built using data lake technology, coupled with Elasticsearch, Kibana, and Spark.

DX Operational Intelligence is available on-premises, as a SaaS solution, hybrid, or delivered by a managed service provider. The code base is common across all implementations, and is based on a microservices and container-based architecture. It is therefore also cloud agnostic, so it works with AWS, Azure, GCP, or IBM Cloud.

The tool gathers data via automated discovery, Broadcom agents, open APIs, and REST-based connectors for other third-party tools. These tools can be pre-built extensible web services, polling, SNMP discovery/MIB integration, JMX syslog, and local log parsing.

Data consumption can use Broadcom and non-Broadcom monitoring tools directly from a data center, cloud assets, CMDBs, ITSMs, and various data types. Data types include CIs, topology, alarms, events, metrics, logs, and wire data. This tool supports both stream and batch processing with sub-second query response times.

The log data analysis ingests unstructured log data with contextual workflows, alerting, and search via Kibana integration. "Log-scraping" agents ingest data from live streams in parsed format and create metrics from pattern matching within log entries.

Strengths: This one is the most improved of all the AIOps tools in this report, with one of the most comprehensive solutions for those running all types of systems such as legacy, network edge, public, and private clouds. The multiple deployment options make it a good fit for those enterprises that have not yet selected a platform for ops tooling.

Challenges: The tool could be too complex for smaller shops and ops teams that may not need all of its features.

Centerity Secure AIOps

Centerity Secure AIOps is an AIOps monitoring tool that analyzes health, performance, and security from a single console. This helps organizations visualize risks and measure them within the proper business context. Secure AIOps provides system visibility, aggregates all, including security and alerts, into unified views, and correlates them to IT incidents as they're identified. This platform can also assess risk, measure resource utilization, and evaluate security posture. It will also present data in customized views.

Secure AIOps delivers these full technology stack views to business service stakeholders. This ensures the health, performance, and security of all digital processes. The concept is to help IT, risk, and security leaders clearly understand the business impact of enterprise issues.

This tool can display real-time business analytics; identify performance and cyber anomalies; and isolate faults across applications, operating systems, hardware infrastructure, and the cloud. It consumes this information from SNMP to Syslog/Logs, RestAPI, WMI, MQTT, and other sources.

Strengths: With a focus on security plus general IT, Centerity has a unique approach that may make this tool more valuable to those that want just one system for IT and security. The solution offers a unified view of IT and security events enhanced with AI, enabling insight into the health of a company and a correlated answer to root-cause issues.

Challenges: The depth of application knowledge and insight is not as great as what other tools in this space have. Many organizations may still need deeper application-focused tools.

Cisco AppDynamics

Cisco AppDynamics focuses on complex deployments with an AIOps monitoring solution. The AppDynamics Cognition Engine applies machine learning (ML) and AI to application performance management (APM), infrastructure monitoring, end-user monitoring, and business performance monitoring. It is clearly application-oriented, with a deep ability to handle enterprise and cloud-based systems.

The AppDynamics APM solution is more business transaction-centric than other tools. It focuses on application and user monitoring, which seems to be missing in many other tools. The tool can proactively identify and then actively or passively mitigate application performance issues.

The APM features provide visibility down to the code level and support heterogeneity across multi-cloud environment transactions. The infrastructure monitoring tool provides a view of connections between applications and infrastructure, whether the application is hybrid cloud, multi-cloud, or on-premises. As with other large vendors, Cisco provides increased value when added to other Cisco solutions.

AppDynamics can ingest data from its own agents, as well as via open standards such as Prometheus and OpenTelemetry. It's an example of an AIOps solution in that it leverages a topology and dependency-aware data model that spans domains. This tool can baseline any number of collected metrics to find a normal state, and the knowledge engine can find anomalies and eliminate them from the baseline. The combination of business awareness and AIOps features makes this a compelling solution.

Strengths: Good fit for mid-sized to large organizations, with an APM focus that supports traditional systems while new features support modern applications and cloud platforms. The addition of Digital Experience Monitoring (DEM), which is a superset of internet and cloud network monitoring from Cisco's ThousandEyes purchase, provides visibility into digital dependencies that impact WAN, cloud computing platforms, and SaaS applications performance.

Challenges: Areas that need improvement include deeper support for Google Cloud Platform and Microsoft Azure. Also, Cisco could improve its approach to handling agents.

CloudFabrix CfxDimensions

CloudFabrix has a well-rounded product suite, which can address broad AIOps use cases including ITOps, NocOps, InfraOps, IT planning and service/delivery for multiple stakeholders. It has made good strides with ease of deployment, with its microservices-based cloud architecture, faster DataOps-based integration with multiple sources, and sinks using robotic data automation, as well as an end-to-end offering for edge to core to cloud, with observability in the box and Cfx Dimensions. The ML model training leverages both historical and real-time data streams, with rich bot and natural language processing (NLP) libraries.

With a focus on asset discovery and intelligence, Cfx Dimensions uses an agentless, multi-protocol approach with remote calls. It has API integration with aggregation/management/monitoring systems like VMware vCenter, SCOM, AppDynamics and so on. It also has API and CLI integrations with systems that can provide flow and connectivity data to help establish topological awareness, such as NetFlow, netstat, AWS flow logs and tracing.

cfxDimensions can process data in the following key areas:

- ITOM sources: Alerts, alarms, and events
- Observability data: Metrics, logs, traces, and flow data
- ITSM: Incidents/trouble tickets from ticketing systems
- CMDB (optional integration): IT asset inventory, services, and mapping
- Unstructured text from tickets and incidents for NLP analytics
- Historical alert/event data for model training
- Change events from ITSM and CI/CD systems

Strengths: CloudFabrix has strong AI and ML capabilities, which enables targeting of a broad set use cases including ITOps, NocOps, InfraOps, IT planning and service delivery. It is a leader in this market due to its strong AI/ML.

Challenges: The process of training the AI can be daunting for companies new to the technology. Most organizations will have a limited set of recent data to feed into the system from historical logs, and providing deeper data and telemetry for effective results requires both investment and time (on the order of one to six months).

Datadog

Datadog is a unified SaaS cloud monitoring and security platform. Datadog monitors systems using an agent and API calls to support containers, VMs, services, databases, storage systems, and network devices. For monitoring parts of your environment that can't accommodate an agent, Datadog can gather information remotely using SNMP, JMX, OpenMetrics, or remote API calls. Datadog also consumes logs, APM, and user experience metrics to enhance intelligence advice.

The Datadog agent runs inside Kubernetes clusters to collect metrics, traces, and logs in real time. The agent is containerized as a sidecar, or agentless deployment using a Lambda layer in serverless environments.

Datadog's approach to gathering network metrics is via a cloud-native network monitoring feature that counts packets between source and destination. Using tagging, it can track dependencies and metrics such as request volume, RTT (round-trip time) variance between persistent components like services or applications, and short-lived components like Kubernetes pods.

The platform offers more than 450 vendor-backed integrations such as AWS Fargate and Lambda, Google Cloud Run and Functions, Azure Functions, and Azure App Service for serverless operations. It also offers orchestrators such as Kubernetes, OpenShift, Amazon ECS and AWS Fargate, Rancher, Mesos, Docker Swarm, Cloud Foundry, and Azure Container Instances.

Strengths: Datadog offers numerous integration services, including all public cloud providers, and a good mix of on-premises and cloud-based systems integrations. Using an agent to collect data reduces the need to leverage a new agent each time data must be acquired. Datadog is a leading contributor to open standards like OpenTelemetry and OpenMetrics, which will radically change the value of AIOps tools.

Challenges: Datadog needs to improve the on premise system AIOps value cases in which an agent can't be deployed. Best value is achieved by adding other AI tools.

Dynatrace Software Intelligence Platform

The Dynatrace platform provides a broad spectrum of connectivity, both traditional and cloud, browser or mobile apps, third-party content providers, back-end services down to code-level, web services and containers, serverless functions (FaaS) database requests, and custom services.

Dynatrace can auto-discover hosts, cloud instances, and containers, including K8S cluster, node and pod health, OpenShift, Cloud Foundry, and VMware. Cloud support includes AWS, Azure, GCP, Alibaba, Oracle, and IBM.

The platform can autodiscover logs and parse metrics for charting, alerting, analytics, and custom metrics/events via APIs. Besides natively monitored systems, Dynatrace can integrate with myriad

other third-party technologies, including open-source agents such as OpenTelemetry, Telegraf, Prometheus, and StatsD.

The platform can store and process the following data types and the relationships and dependencies:

- Metrics (time series)
- Events and log data
- Transactional traces
- Code-level details along the traces (such as PurePath)
- User actions and sessions
- Monitored entities (host, processes, services, and applications) and dependencies between them (such as Smartscape)
- Metadata

Dynatrace uses a built-in context mode called Smartscape to automatically store all data and events acquired by the instrumentation and integration with external sources. Smartscape can leverage more than 130 built-in entity types, such as host, container, process, service, function, POD, and more. The model is also extensible, so customers and partners can provide additional technology support.

Dynatrace has a causation-based AIOps engine, Davis, that provides multi-dimensional analytics. It automatically processes billions of dependencies in real-time, continuously monitors the full stack for system degradation and performance anomalies, and delivers precise answers with root-cause determination, prioritized by business impact. The Dynatrace Davis Assistant enables chat box and voice interaction. Dynatrace Davis data units allow for a currency that can be extended as business needs grow, enabling scale and maximum value. Following an industry trend on how to monetize software that is customer-friendly, the units can be repurposed so the business can optimize the value of the credits to fill the needs at that time.

Strengths: The ability to provide detailed AIOps services for a wide range of platforms, as well as other enterprise integrations, makes Dynatrace one of the more comprehensive solutions in this report. For many enterprises, Dynatrace could provide a one-stop shop solution.

Challenges: The implementation effort for this product is more difficult when you can't deploy the Dynatrace OneAgent to entities you need to monitor. Setup of this AIOps solution might require a steeper learning curve for large ops teams that are accustomed to event correlation and not full-stack analysis. While the solution provides value out of the box, most buyers, including users we interviewed, may require additional configuration to match their business logic and specific workflows.

IBM Cloud Pak for Watson AIOps with Instana

The IBM Watson AIOps solution can discover components through a variety of methods, including using agents, SNMP, API integration, network discovery, port scanning, and other proprietary interfaces. This tool can monitor structured or unstructured data such as events, time series data, application logs, system logs, data flow, configuration, application or service topology, tickets, alerts, and other metrics.

Leveraging the Watson engine, this IBM tool has strong AI capabilities for NLP, fault localization, event correlation and linking, anomaly detection, and incident matching. There are more than 250 integrations via APIs. The tool supports industry vendors and universal connections through Webhook, email, SNMP, REST, file, and so on.

The process is focused on ease of use. Non-technical users can create their own dashboards with drag and drop functionality. It also supports most other reporting and dashboard types, such as heatmaps, time series, histograms, service level objectives, AI model health, and others. It also provides ChatOps and automatic ticket creation.

There is integration with just about any alerting tool via API integration. IBM Cloud Pak for Watson AIOps (CP4WA) provides native alerting and notification through the platform UX and team ChatOps. This tool uses ML and natural language processing to perform alert grouping and triaging analysis.

Strengths: Watson AIOps provides a comprehensive approach to AIOps, with full enterprise monitoring and management. It's an E2E platform that addresses complex, mission-critical use cases across the overlapping AIOps and management spaces, including incident management, observability, governance and compliance, efficiency and cost management, hybrid application management, and others.

Challenges: As with other comprehensive AIOps tools, deployment can be complex. This tool may be a challenge for many enterprise ops shops to set up while it may be overkill for small to midsize companies. Existing IBM customers would be unlikely to have the same difficulty.

Micro Focus Operations Bridge

Micro Focus Operations Bridge (OpsBridge) AIOps solution is built on a common platform with other Micro Focus ITOM products, which means it can integrate service management, brokering, and asset management. This tool is based on container, orchestration, and micro-service technologies focusing on IT operations management functions.

OpsBridge is built atop the OPTIC platform, which provides a single framework for managing data collection and storage in a common data lake built on Vertica. OPTIC can optimize resources, processing power, and network loads, making this one of the more unique approaches for AIOps.

This tool can harness best practices and apply automation across discovery, monitoring, analytics, and remediation. This prebuilt or able-to-build approach helps with the AIOps deployment process.

The OpsBridge solution automatically monitors and analyzes the health and performance of multi-cloud and on-premises resources across devices, operating systems, databases, applications, and services on all data types. The platform provides event consolidation, correlation engines, and big data analytics-based noise reduction. It integrates end-to-end service awareness with rule and machine learning-based event correlation delivered on top of a data lake.

Strengths: The strong legacy system approach, combined with more modern systems ops such as cloud, edge, and IoT, makes this one of the more comprehensive tools. A Global 2000 enterprise could leverage just this tool for most of traditional ops. The CloudOps aspect of this tool has been much improved since last reviewed.

Challenges: As with other comprehensive AIOps tools, there could be a potentially complex deployment. It may be a challenge for many enterprise ops shops and may be overkill for small to midsize companies.

Moogsoft AIOps

The Moogsoft AIOps platform helps automate service assurance for both on-premises and cloud-based systems. This tool can analyze billions of events every day both in and between complex deployments, such as multi-cloud and hybrid cloud.

Moogsoft leverages AI to provide a layer of intelligence for detecting and automating resolution of ops issues. Unlike other tools evaluated in this report, Moogsoft AIOps takes a *workflow approach* to ops by defining how to spot and correct issues within a logical task group.

Users can filter data and events coming in from managed systems, and direct data to the appropriate processes and ops staffers. The idea is to establish a system that does not “cry wolf” and instead alerts ops only to critical events requiring human intervention.

With this approach, noisy alerting systems are monitored but not always acted upon. The tool correlates alerts and groups and acts only on those that need resolution. This approach examines the root causes and prescribes a solution. Moogsoft AIOps works well with others and provides out-of-the-box integration with security systems and DevOps tool chains. For example, Moogsoft can detect a problem and create a bug ticket in Jira, then inspect a staffing tool like PagerDuty or xMatters to identify an available on-call person and inform them of the Jira bug ticket. Moogsoft then continues to monitor the incident, closing out the ticket once the incident is resolved.

Strengths: This tool provides good use of machine learning, as well as root cause analysis. The AI in Moogsoft is particularly strong in finding correlations between seemingly unrelated data. Moogsoft has the ability to ingest data from any source becoming stronger as more data are consumed. There

are also integrations with other tools, including DevOps and security tools.

Challenges: This tool is lacking some resolution automation services, as reported by Moogsoft users. The ability to ingest any data from any source can make integration challenging as the possibilities may be daunting for IT shops with lower maturity.

Nastel XRay (and the Nastel platform)

Nastel connects to any source of machine data, and maintains a library of supported connectors it makes available to customers via github. Nastel has strong support for the banking industry, supporting for example, Dodd-Frank compliance in the United States and Securities Financing Transactions Regulation (SFTR) in the European Union. It also provides connectors for many popular log file formats.

Nastel provides a schema to define new models, creates them, and makes them available to customers. The Nastel tools also use several AI algorithms to ensure it can discover signals in any relationships.

There are a number of interfaces provided, including an API that allows for integration into any ops tools. The tool also leverages Docker for installation, Kubernetes for orchestration, and several others. The jKQL natural language query language is aimed at the complexity problem in large-scale enterprise applications. This query language allows for a normalization that enables enterprise messaging versatility.

Nastel employs a visual dashboard UI, and lets users create live views exposed as iframes and URLs for inclusion in other dashboards. This customization is becoming a common requirement for those leveraging AIOps.

XRay and the Nastel platform can automate corrective and preventative actions. The tool integrates with ticketing systems and event management systems. The solution can be deployed on premise, in the cloud, or as a SaaS offering.

Strengths: 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. Provides peerless awareness of middleware message flows.

Challenges: The downside of having a more extensible framework is the 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.

New Relic One

New Relic One is a cloud-based observability platform that provides full AIOps, APM, infrastructure, log management, real-user monitoring via an agent in the browser (RUM), synthetics traffic injection by remote bots, mobile agent code for mobile support, and native client monitoring via agents.

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.

New Relic One provides integration with Amazon Web Services, Google Cloud Platform, and Microsoft Azure. It connects these cloud providers to its Telemetry Data Platform, Full-Stack Observability, and Applied Intelligence products. The platform supports hybrid environments and container orchestration systems, including Kubernetes, AWS ECS, AWS EKS, AWS Fargate, Azure Container Service, Google Kubernetes Engine, Anthos, PCF, PKS, RedHat OpenShift, Rancher, and Docker Swarm.

The Kafka-based architecture is designed to scale. It can ingest two billion data points per second and allows for a degree of latency. Data received can be up to 24 hours old. Users can send data from the New Relic platform to AWS as a limited feature release for long-term storage and data mining purposes via an API.

Strengths: Intuitive visualization provides quick and easy insight into systems. Tags help users create dashboards with little IT intervention and the platform is built to scale. The IoT via synthetic transactions provides extended value to buyers needing to support IoT and Edge deployments.

Challenges: Despite several AI features, New Relic One is not able to provide the same level of AI functionality as other vendors in this report.

OpsRamp AIOps

OpsRamp AIOps focuses on event and alert management—an approach that helps abstract operational staffers from a confusing amount of data. OpsRamp delivers real-time context by combining event data with topology information in a business-service map, so that IT operations teams can understand the criticality of a particular service degradation and take appropriate action.

OpsRamp can perform unified data analysis to determine holistic patterns. This includes determining the root cause of an issue and starting instantaneous remediation.

As far as monitoring public clouds goes, this AIOps platform identifies issues in and around cloud deployments in real-time. This includes intelligent management, which helps enterprises abstract multi-cloud complexity, as well as simultaneously monitoring legacy environments.

OpsRamp can handle growing volumes of alerts and events with automated event correlation. This means you can group events, such as networking and system, and limit the amount of data you must sort through. This helps users view actionable conclusions for most incidents and ignore false alarms.

The business connection is unique to OpsRamp. It provides visibility into business service impact via contextual alerts. It also provides real-time analytics that help determine the root causes of problems.

Strengths: OpsRamp can collect and analyze fine-grained operational data using dynamic dashboards.

Challenges: Using agents to gather data may make deployment more complex. Using agentless data collection requires the target to support an API and a gateway process (proxy) for them to get this data from behind firewalls or network-based security controls. This is a common problem for SaaS-based solutions that must be accounted for.

Splunk AIOps

Splunk's IT Service Intelligence (ITSI) module is part of the overall Splunk AIOps solution. This module is part of Splunks premium solutions that can be purchased as add ons and leverages the core part of Splunk which comes with Splunk Enterprise or Splunk Cloud purchase.

The overall Splunk AIOps solution combines monitoring, troubleshooting, and incident-response solutions that boost application modernization initiatives. Splunk achieves this by using open data collection, streaming analytics, and machine learning. Splunk's goal is to maximize service resilience and performance over time. It combines infrastructure monitoring, application performance monitoring, digital experience monitoring, log investigation, and incident response into a single solution. Specifically, Splunk is able to help operations teams collect any data, identify anomalies across the stack, aggregate and prioritize alarms into notable incidents to reduce alert noise, respond to incidents quickly, diagnose their root cause, and implement recommended remediations.

Splunk IT Service Intelligence (ITSI) is built on the Splunk platform and requires either Splunk Cloud or Splunk Enterprise. ITSI ingests and correlates events and alerts from multiple data sources (other tools, systems, applications, and the like), creating meaningful "episodes" (a Splunk term) based on aggregation policies and ML algorithms. ITSI can execute actions on episodes automatically using aggregation policies, such as sending an email, pinging a host, or creating a ticket in a third-party system.

ITSI uses machine learning algorithms to predict the health score value of a selected service using historical service health scores and KPI data to approximate what a service's health might look like in 30 minutes. The ITSI AIOps capabilities include predictive analytics, adaptive thresholds, and anomaly detection. ITSI also includes clustering of related alerts into a single incident as an intelligent way to reduce noise and correlate events.

Other Splunk products can be leveraged for AIOps use cases including Splunk IT Essentials and no-cost Splunkbase applications. Other Splunk tools for use with ITSI are Splunk Infrastructure Monitoring, Splunk APM, Splunk RUM (real user monitoring), Splunk Synthetic Monitoring, Splunk Log Observer, and Splunk On-Call.

Splunk Infrastructure Monitoring, Splunk APM, Splunk RUM and Splunk Log Observer are available as standalone SaaS solutions, or pre-packaged and integrated via the Splunk Observability Cloud.

Splunk has a wide range of integrations available at splunkbase.splunk.com to aid root cause analysis and resolution. Examples include ServiceNow, IBM Z Decision Support, Jira, SolarWinds, Git, Jenkins, Spinnaker, GitLab, and Circle CI. The integrations provide a broad selection of visualizations and easy access to logs, metrics, and traces to facilitate diagnosis and remediation.

There are dashboards out of the box for common use cases, but ITSI also enables the creation of custom dashboards in which the unique KPIs of a business or technical service can be incorporated into custom views.

Splunk's solutions are subscription-based pricing models. There are two pricing models—host-based and usage-based. Customers can purchase products standalone or as cloud-based suites, paying on a monthly or annual basis.

Strengths: Splunk ingests full-fidelity data from all sources (logs, metrics, and traces) across the full stack and supports real-time data with streaming ingestion. Splunk also provides massive scalability, sophisticated in-stream analytics, native OpenTelemetry support (an emerging standard to which Splunk is a major contributor), and AI/ML features throughout its solution.

Challenges: Some customers expressed concerns about the cost and potential difficulty of migrating to Splunk IT Service Intelligence as it requires Splunk Enterprise or Splunk Cloud to be deployed and integrated first. Even discounted, the overall cost could be more expensive in the long run compared to other vendors reviewed when only focusing on AIOps costs.

6. Analyst's Take

A core takeaway from this report is: the number of AIOps providers is increasing, as more traditional enterprise players jump into the ring and more traditional ops players AI-enable their solutions. There will be many vendors providing different types of tools with different approaches aimed at different market sectors.

We are beginning to see some emerging order out of this confusion, evolving around two general types of AIOps providers. The first are enterprise-focused vendors that offer more comprehensive solutions. These are the tools that support most of the systems in use at large enterprises, including traditional systems, cloud, and emerging models such as edge and IoT.

While some of the vendors in this group can provide one-stop-shopping for AIOps, supporting most enterprise ops as well, they do so in different ways. Some move from the cloud down to on-premises, while others attack the challenge from the other direction.

The second group is particularly intriguing, and comprises niche players. Security ops focused AIOps, as well as those that focus on FinOps and other operational spaces, are beginning to emerge. While a few are covered here, most are emerging and may not even call themselves AIOps tools, yet they clearly provide AI and predictive analytics.

Our conclusion is that AIOps will evolve as a stack of tools, instead of a single tool. This stack likely will consist of a foundational tool, such as those provided by IBM, Dynatrace, or Micro Focus; along with other tools that would provide operational features for specific types of systems, such as IoT, finance, and security. This approach may create a new industry of tool stacks from each company, sold together, or more likely, larger companies purchasing the niche AIOps tools to complete their own stack.

Keep in mind that many of these technologies are at least one year old, and are more mature than the new buzzwords would lead you to believe. There seem to be layers within most of these tools. The older technology is doing most of the heavy lifting, with layers of new technology providing integration with newer systems such as cloud and edge computing.

Changes that will be driving the 2022 report will include emerging standards, OpenCensus merging with OpenTracing to form OpenTelemetry, OpenMetrics, and OpenID Connect. OpenTelemetry and OpenMetrics are directly related to operational monitoring and OpenID Connect is a common identification process that makes security easier to manage when systems must be able to connect to each other to get operational awareness data. OpenCensus and OpenTracing are merging into OpenTelemetry, which will be run as a CNCF project. OpenMetrics is a vendor-neutral way for systems to expose operational data (aka metrics) and is an IETF project. OpenTelemetry will focus on monitoring at scale end to end while OpenMetrics will focus on a standard way to expose operational data at scale.

As vendors either adapt or migrate to the new standard in 2021, the impact will be a game changer in 2022. While these standards are independent of AIOps, they address the issue of how to get data into an AIOps engine, which today is labor intensive.

We can consider the AIOps space as a relaunch of traditional operational tools. They are able to manage most of what we're finding now within the enterprise. This will be a required weapon as the battle to deal with IT complexity becomes more difficult and more urgent across the enterprise.

7. About David Linthicum

David Linthicum is an internationally renowned thought leader in cloud computing. He has spent the last 25 years teaching large global enterprises across all industries how to use technology resources more productively and to constantly innovate.

David has been a CTO five times for both public and private companies, and a CEO twice. He has published 13 books on computing and his thought leadership pieces have appeared in the Wall Street Journal, NPR, Forbes, InfoWorld and Lynda.com. He has worked with both startups and established corporations to expand their vision of the possible and the achievable.

8. About 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.

9. About Michael Delzer

Michael Delzer is a global leader with extensive and varied experience in technology. He spent 15 years as American Airlines' Chief Infrastructure Architecture Engineer, and delivers competitive advantages to companies ranging from start-ups to Fortune 100 corporations by leveraging market insights and accurate trend projections. He excels in identifying technology trends and providing holistic solutions, which results in passionate support of vision objectives by business stakeholders and IT staff. Michael has received a gold medal from the American Institute of Architects.

Michael has deep industry experience and wide-ranging knowledge of what's needed to build IT solutions that optimize for value and speed while enabling innovation. He has been building and operating data centers for over 20 years, and completed audits in over 1,000 data centers in North America and Europe.. He currently advises startups in green data center technologies.

10. 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.

11. Copyright

© Knowingly, Inc. 2021 *"GigaOm Radar for AIOps Solutions"* is a trademark of Knowingly, Inc.. For permission to reproduce this report, please contact sales@gigaom.com.