



Ron Williams
Mar 20, 2024

GigaOm Radar for Cloud Observability ^{v4.01}

Table of Contents

- [1. Executive Summary](#)
- [2. Market Categories and Deployment Types](#)
- [3. Decision Criteria Comparison](#)
- [4. GigaOm Radar](#)
- [5. Solution Insights](#)
- [6. Analyst's Outlook](#)
- [7. Methodology](#)
- [8. About Ron Williams](#)
- [9. About GigaOm](#)
- [10. Copyright](#)

1. Executive Summary

Cloud observability is the process of gaining comprehensive insights into the performance, health, and state of cloud-based applications and infrastructure through monitoring, metrics, tracing, logging, and other telemetry data. It enables organizations to proactively detect, understand, and resolve issues to ensure optimal application performance and user experience.

Observability is one step in a larger operational intelligence workflow wherein organizations move from *monitoring* to *observability* to *intelligence* (**Figure 1**).

Monitoring can determine the states of various hardware or software resources. Observability enables the consolidation of these states to obtain meaning, estimate the impact on critical services, predict future states based on past observations, and automatically remediate known problems. Intelligence synthesizes both technical information and business data.

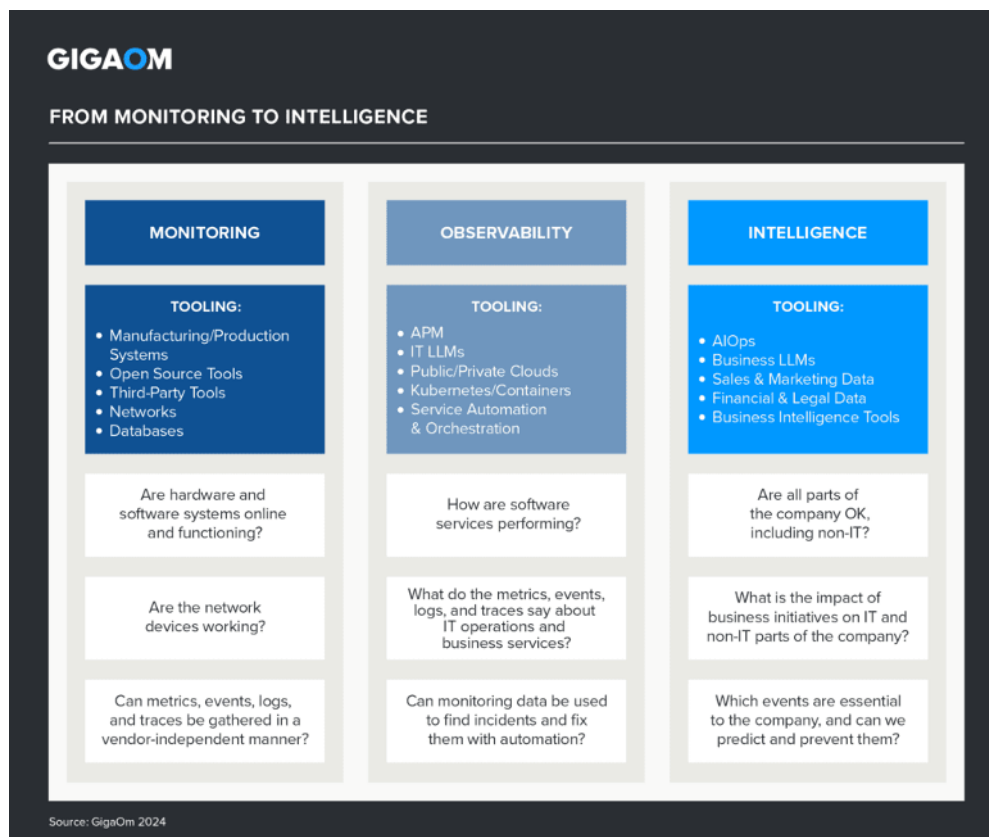


Figure 1. From Monitoring to Intelligence

Observability tools reduce the data overload and bring insight to the monitored data. These solutions leverage application performance management (APM), service orchestration and automation, Kubernetes management, and cloud provider tooling (for public clouds) and apply machine learning (ML) capabilities and predictive analytics to filter the monitored data. The resulting information is targeted at IT operations and other technical personnel such as developers and systems managers. IT operations staff no longer have to be experts on the software and hardware that run the enterprise. With predictive analytics, IT resources can concentrate on what is failing and what is likely to have problems. Additionally, the use of OpenTelemetry gives enterprises a source for metrics, events, logs, and traces (MELT) that is vendor-agnostic.

Intelligence is the final step in this process—it reflects the operational state of the entire company. Intelligence builds on monitoring and observability and begins to deliver on the promise of artificial intelligence for IT operations (AIOps) by including data from the entire company—marketing, sales, legal, human resources, manufacturing data, and other sources.

The history of IT is filled with products and services deemed to be smart or intelligent— hardware and software initiatives, application solutions, databases, and others, often, however, not much more than marketing terms. In 2023, large

language models (LLMs) exploded—spearheaded by OpenAI and ChatGPT—creating the beginning of actual intelligent software. This new ability is finding its way into IT solutions and complicates the definition of observability versus intelligence.

The focus of this analysis will be on observability within cloud environments, including multiple public cloud offerings, private clouds, and any combination of cloud and on-premises operations. LLM-driven capabilities will be considered from a “this is new” perspective and an understanding that LLM abilities are inconsistent across all vendors.

This is our fourth year evaluating the cloud observability space in the context of our Key Criteria and Radar reports. This report builds on [previous analysis](#) and considers how the market has evolved over the last year.

This GigaOm Radar report examines 21 of the top cloud observability solutions and compares offerings against the capabilities (table stakes, key features, and emerging features) and nonfunctional requirements (business criteria) outlined in the companion Key Criteria report. Together, these reports provide an overview of the market, identify leading cloud observability offerings, and help decision-makers evaluate these solutions so they can make a more informed investment decision.

GIGAOM KEY CRITERIA AND RADAR REPORTS

The GigaOm Key Criteria report provides a detailed decision framework for IT and executive leadership assessing enterprise technologies. Each report defines relevant functional and nonfunctional aspects of solutions in a sector. The Key Criteria report informs the GigaOm Radar report, which provides a forward-looking assessment of vendor solutions in the sector.

2. Market Categories and Deployment Types

To help prospective customers find the best fit for their use case and business requirements, we assess how well cloud observability solutions are designed to serve specific target markets and deployment models (**Table 1**).

For this report, we recognize the following 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 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.

- **Cloud service provider (CSP):** Providers delivering on-demand, pay-per-use services to customers over the internet, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

In addition, we recognize the following deployment models:

- **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 advantage of this type of solution is the integration with other services offered by the cloud service provider (functions, for example) and its resulting simplicity.
- **On-premises:** These solutions are deployed on customer-owned infrastructure and managed by the enterprise.
- **Hybrid:** These solutions are meant to be installed both on-premises and in the cloud, allowing organizations to build hybrid or multicloud infrastructures. Integration with a single cloud provider could be limited compared to the other options and more complex to deploy and manage. On the other hand, this approach is more flexible and the user usually has more control over the entire stack regarding resource allocation and tuning.

Table 1. Vendor Positioning: Target Market and Deployment Model

GIGAOM			
VENDOR POSITIONING: TARGET MARKET AND DEPLOYMENT MODEL			
	TARGET MARKET		
	SMB	Large Enterprise	
AWS	✓	✓	
BMC	—	✓	
Broadcom	✓	✓	
Chronosphere	✓	✓	
Cisco	✓	✓	
CloudFabrix	—	✓	

Datadog	✓	✓	
Dynatrace	✓	✓	
Elastic	✓	✓	
Grafana	✓	✓	
Honeycomb	✓	✓	
IBM	✓	✓	
LogicMonitor	✓	✓	
Microsoft	✓	✓	
New Relic	✓	✓	
OpenText	—	✓	
ServiceNow	✓	✓	
SolarWinds	✓	✓	
Splunk	✓	✓	
StackState	✓	✓	
Sumo Logic	✓	✓	

Source: GigaOm 2024

Table 1 components are evaluated in a binary yes/no manner and do not factor into a vendor’s designation as a Leader, Challenger, or Entrant on the Radar chart (**Figure 2**).

“Target market” reflects which use cases each solution is recommended for, not simply whether that group can use it. For example, if an SMB could use a solution but doing so would be cost-prohibitive, that solution would be rated “no” for SMBs.

3. Decision Criteria Comparison

All solutions included in this Radar report meet the following table stakes—capabilities widely adopted and well implemented in the sector:

- Infrastructure discovery and performance monitoring
- Application performance monitoring
- Network performance monitoring
- Cloud resource utilization
- Data enrichment
- OpenTelemetry support

Tables 2, 3, and 4 summarize how each vendor included in this research performs in the areas we consider differentiating and critical in this sector. The objective is

to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the relevant market space, and gauge the potential impact on the business.

- Key features differentiate solutions, outlining the primary criteria to be considered when evaluating a cloud observability solution.
- Emerging features show how well each vendor is implementing capabilities that are not yet mainstream but are expected to become more widespread and compelling within the next 12 to 18 months.
- Business criteria provide insight into the nonfunctional requirements that factor into a purchase decision and determine a solution's impact on an organization.


These decision criteria are summarized below. More detailed descriptions can be found in the corresponding report, "[GigaOm Key Criteria for Evaluating Cloud Observability Solutions](#)."

Key Features

- **Dashboards and reporting:** Whether premade or custom, reports are a key feature of cloud observability solutions, and all solutions will have some capabilities in this area. Reports must include performance, monitoring, utilization, and (if possible) prediction. What will differentiate solutions here is the ease with which users can customize and share dashboards, along with templates that enable easy customization.
- **User interaction performance monitoring:** In cloud observability, the performance value of an application is based on how well user needs are handled through real user monitoring (RUM), synthetic monitoring, and transaction tracing. User interaction performance monitoring looks at every part of a cloud application that a user may touch, wherever it may reside, whether in a single cloud or multiple clouds, both public and private.
- **Multicloud functionality:** The allocation and provisioning of resources from multiple clouds are important features for larger organizations. This criterion looks at whether a solution can see multiple cloud instances and how cloud resources are displayed. Solutions should be able to provide this information via individual reports or through a single display with all cloud resources shown. Leading solutions often provide the latter.
- **LLM support:** The past 12 months have seen an increasing prevalence of LLMs as a way of interfacing with existing performance data, offering insights, and proposing resolution options. Vendors' current capabilities vary greatly. Some LLMs can respond with a chart, a line graph, or data. Others have links to an external LLM. Another can observe connections to an LLM and log the inputs and outputs to allow the business to understand the data used by an external LLM.
- **Pushing and tagging data:** Metrics, logs, and other monitoring data need to be collated, pushed to a server, and then tagged in terms of its source, timestamp, and so on. This adds context to downstream analysis, supporting better identification, scoping, and diagnosis of issues.

- Predictive analysis:** This criterion looks at the ability of solutions to predict usage trends and generate alerts about pending incidents. IT and business personnel alike benefit from having insight into the future—for example, the prediction of a load spike that does not correspond to a known business event or the prediction of a memory problem in a critical service. Leading solutions offer strong predictive capabilities.

Table 2. Key Features Comparison

		KEY FEATURES COMPARISON														
<table border="1"> <tr><td>★★★★★</td><td>Exceptional</td></tr> <tr><td>★★★★</td><td>Superior</td></tr> <tr><td>★★★</td><td>Capable</td></tr> <tr><td>★★</td><td>Limited</td></tr> <tr><td>★</td><td>Poor</td></tr> <tr><td>—</td><td>Not Applicable</td></tr> </table>		★★★★★	Exceptional	★★★★	Superior	★★★	Capable	★★	Limited	★	Poor	—	Not Applicable	AVERAGE SCORE	KEY FEATURES	
★★★★★	Exceptional															
★★★★	Superior															
★★★	Capable															
★★	Limited															
★	Poor															
—	Not Applicable															
	Dashboards & Reporting	User Interaction Performance Monitoring														
	↕	↕	↕													
AWS	3.3	★★★★★	★★★★													
BMC	3.7	★★★★★	★★★★													
Broadcom	3.5	★★★	★★★★★													
Chronosphere	2.5	★★★★	★★★★													
Cisco	3.8	★★★★★	★★★★★													
CloudFabrix	3.7	★★★	★★★★													
Datadog	3.8	★★★★★	★★★★★													
Dynatrace	4.5	★★★★★	★★★★★													
Elastic	3	★★★★	★★★★													
Grafana	3.3	★★★★★	★★★★													
Honeycomb	3	★★★★★	★★★★													
IBM	3.2	★★★★★	★★★★★													
LogicMonitor	3.2	★★★	★★★★													
Microsoft	2.8	★★★★	★★★★													
New Relic	3.8	★★★★★	★★★★★													
OpenText	3.3	★★★★★	★★★★★													
ServiceNow	2.3	★★★★★	★★★★													
SolarWinds	3.3	★★★★★	★★★★													

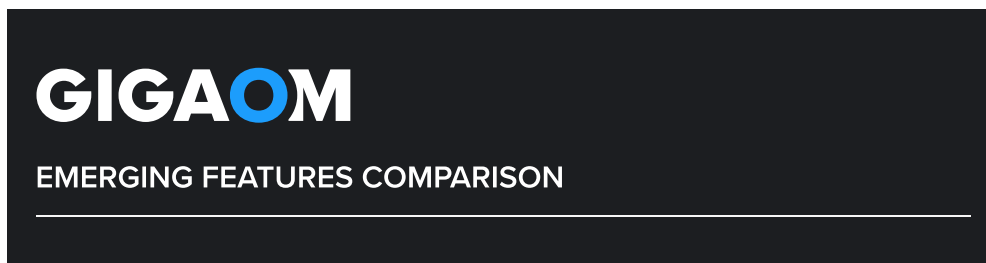
		KEY FEATURES		
★★★★★ Exceptional ★★★★ Superior ★★★ Capable ★★ Limited ★ Poor – Not Applicable	AVERAGE SCORE			
		↔	↓↑	↓↑
		Dashboards & Reporting	User Interaction Performance Monitoring	
Splunk	3.5	★★★★★	★★★★★	
StackState	2.8	★★★★★	★★★	
Sumo Logic	2.7	★★★★★	★★	

Source: GigaOm 2024

Emerging Features

- Edge observability:** Given the increased importance of applications that run at the edge or include some edge data collection or processing, cloud observability also needs to take into account these extended workloads. A continuing trend is to use distributed AI/ML on edge infrastructure.
- Identification of ghost changes:** When integrated with other IT operations management tools, cloud observability solutions provide visibility into scheduled changes. But there are often other changes that do not go through a formal change management process. These are called ghost or shadow changes. Vendors developing capabilities around identifying ghost changes may take cloud observability into new areas of operational awareness.

Table 3. Emerging Features Comparison



		EMERGING FEATURES													
<table border="1"> <tr><td>★★★★★</td><td>Exceptional</td></tr> <tr><td>★★★★</td><td>Superior</td></tr> <tr><td>★★★</td><td>Capable</td></tr> <tr><td>★★</td><td>Limited</td></tr> <tr><td>★</td><td>Poor</td></tr> <tr><td>–</td><td>Not Applicable</td></tr> </table>	★★★★★	Exceptional	★★★★	Superior	★★★	Capable	★★	Limited	★	Poor	–	Not Applicable	AVERAGE SCORE	Edge Observability	Identification of Ghost Changes
	★★★★★	Exceptional													
★★★★	Superior														
★★★	Capable														
★★	Limited														
★	Poor														
–	Not Applicable														
↕	↕	↕													
AWS	3	★★★★★	★												
BMC	2	★★	★★												
Broadcom	2.5	★★★★	★★												
Chronosphere	1.5	★★	★												
Cisco	2	★★★★	★												
CloudFabrix	2.5	★★★★★	★												
Datadog	1.5	★★	★												
Dynatrace	1.5	★★	★												
Elastic	1.5	★★	★												
Grafana	1.5	★★	★												
Honeycomb	2.5	★★★★★	★												
IBM	3	★★★★	★★★★												
LogicMonitor	3	★★	★★★★★												
Microsoft	2.5	★★	★★★★												
New Relic	2.5	★★★★★	★												
OpenText	2	★★★★	★												
ServiceNow	0.5	★	–												
SolarWinds	3.5	★★★★	★★★★★												
Splunk	3.5	★★★★★	★★												
StackState	2.5	★★★★	★★												
Sumo Logic	1.5	★★	★												



Source: GigaOm 2024


Business Criteria

- Ease of deployment:** This criterion looks at how quickly and easily the solution can be deployed and relevant metrics and reports reviewed. When an API is necessary to achieve some significant aspect of the solution, the

integration methods and level of documentation can affect deployment ease.

- **Ease of use:** This criterion looks at how easy it is for users to interact with the solution on a daily basis. Considerations include the consistency of the UI between modules, the ability to share data with other users, and the ease of enabling a user within the software.
- **Agility:** Agility encompasses ease of scaling, which coding environments are supported via what methods, and the number and types of cloud environments supported out of the box (the more public cloud environments supported, the more agile the solution).
- **Ecosystem:** Cloud observability solutions inherently need to work with a wide variety of application stacks, third-party platforms, and multicloud infrastructure environments. They also require configuration based on a complex architecture, perhaps requiring third-party assistance and support. Therefore, the provider’s ecosystem of online documentation, training, certifications, providers, partners, and professional services is important to ease deployment and provide overall solution value.
- **Security:** This encompasses a solution’s ability to mask personally identifiable information (PII) and payment card information (PCI), to keep this data private and abide by compliance and regulatory directives, and to provide single-sign-on (SSO) integration. How the solution handles these requirements, such as via role-based access controls (RBAC), is important.
- **Cost:** Cost includes licensing and professional service needs. Less flexible licensing is generally less complex, but this may come at a great cost. In contrast, highly flexible licensing may create better controls on costs, though with added complexity.

Table 4. Business Criteria Comparison

		BUSINESS CRITERIA COMPARISON													
		BUSINESS CRITERIA													
<table border="1"> <tr><td>★★★★★</td><td>Exceptional</td></tr> <tr><td>★★★★</td><td>Superior</td></tr> <tr><td>★★★</td><td>Capable</td></tr> <tr><td>★★</td><td>Limited</td></tr> <tr><td>★</td><td>Poor</td></tr> <tr><td>–</td><td>Not Applicable</td></tr> </table>	★★★★★	Exceptional	★★★★	Superior	★★★	Capable	★★	Limited	★	Poor	–	Not Applicable	AVERAGE SCORE	Ease of Deployment	Ease of Use
	★★★★★	Exceptional													
★★★★	Superior														
★★★	Capable														
★★	Limited														
★	Poor														
–	Not Applicable														
↔	↓↑	↓↑													
AWS	3.7	★★★★★	★★★												
BMC	3.7	★★★★★	★★★★★												
Broadcom	3.5	★★★	★★★												

		BUSINESS CRITERIA													
<table border="1"> <tr><td>★★★★★</td><td>Exceptional</td></tr> <tr><td>★★★★</td><td>Superior</td></tr> <tr><td>★★★</td><td>Capable</td></tr> <tr><td>★★</td><td>Limited</td></tr> <tr><td>★</td><td>Poor</td></tr> <tr><td>–</td><td>Not Applicable</td></tr> </table>	★★★★★	Exceptional	★★★★	Superior	★★★	Capable	★★	Limited	★	Poor	–	Not Applicable	AVERAGE SCORE		
	★★★★★	Exceptional													
	★★★★	Superior													
★★★	Capable														
★★	Limited														
★	Poor														
–	Not Applicable														
	Ease of Deployment	Ease of Use													
↕	↓↑	↓↑													
Chronosphere	3.2	★★★★	★★★★												
Cisco	3.7	★★★★★	★★★★★												
CloudFabrix	3.2	★★★★	★★★★★												
Datadog	3.8	★★★★★	★★★★★												
Dynatrace	3.8	★★★★★	★★★★												
Elastic	3	★★★★	★★★★												
Grafana	3.2	★★★★	★★★★												
Honeycomb	3.3	★★★★	★★★★★												
IBM	4	★★★★★	★★★★★												
LogicMonitor	3	★★★★	★★★★												
Microsoft	3.8	★★★★★	★★★★★												
New Relic	4	★★★★★	★★★★★												
OpenText	3.7	★★★★★	★★★★★												
ServiceNow	3.8	★★★★★	★★★★												
SolarWinds	3.7	★★★★	★★★★★												
Splunk	3.8	★★★★	★★★★★												
StackState	3.5	★★★★★	★★★★★												
Sumo Logic	3	★★★★	★★★★												

Source: GigaOm 2024

4. GigaOm Radar

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 arrowhead that projects each solution’s evolution over the coming 12 to 18 months.

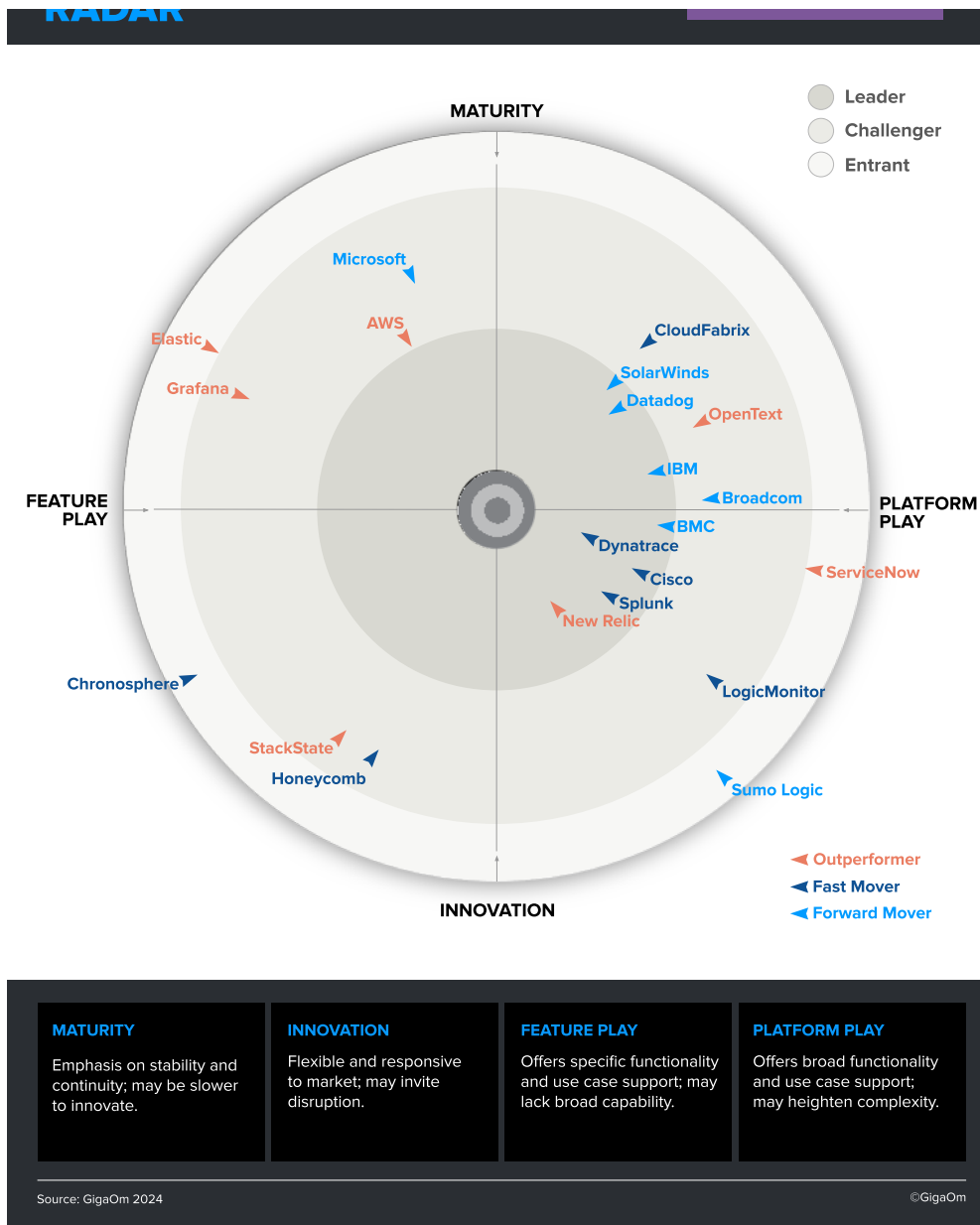


Figure 2. GigaOm Radar for Cloud Observability

Vendor solutions are plotted on the GigaOm Radar chart based on their aggregate scores (across key features, emerging features, and business criteria) and relative to the other vendors in the evaluation. Higher-scoring solutions are positioned closer to center across the Leader, Challenger, and Entrant tiers.

This is the fourth year we've reviewed the cloud observability space, and there are several changes in vendor positioning compared to last year's report. These changes can be attributed to a number of factors, specifically GigaOm [moving from a 0-3 to a 0-5 scoring scale](#), as well as modifying the decision criteria we evaluated. For example, we've added LLM support as a key feature, added edge observability as an emerging feature, added security and cost as business criteria, and we've removed or updated key features and business criteria as well.

As you can see in the Radar chart in **Figure 2**, this year the Platform Play vendors are fairly evenly split between the Maturity and Innovation halves. This represents the change in innovation rates among these vendors and the arrival of mainstream LLM-driven capabilities. The impact of LLMs is significant in this space, and some

vendors that were Leaders in last year's evaluation have moved back into the Challenger or Entrant rings.

Outperformers appear in all quadrants, a distribution that promises many changes and improvements in the next 12 to 24 months. Additionally, there are more Forward Movers this year, indicating that some vendors have been slower to adapt to the changes in the market.

In reviewing solutions, it's important to keep in mind that there are no universal "best" or "worst" offerings; there are aspects of every solution that might make it a better or worse fit for specific customer requirements. Prospective customers should consider their current and future needs when comparing solutions and vendor roadmaps.

INSIDE THE GIGAOM RADAR

To create the GigaOm Radar graphic, key features, emerging features, and business criteria are scored and weighted. Key features and business criteria receive the highest weighting and have the most impact on vendor positioning on the Radar graphic. Emerging features receive a lower weighting and have a lower impact on vendor positioning on the Radar graphic. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and roadmaps.

Note that the Radar is technology-focused, and business considerations such as vendor market share, customer share, spend, recency or longevity in the market, and so on are not considered in our evaluations. As such, these factors do not impact scoring and positioning on the Radar graphic.

For more information, please visit our [Methodology](#).

5. Solution Insights

Amazon Web Services (AWS): CloudWatch

Solution Overview

Amazon's observability tool is CloudWatch, which works with other Amazon tools, including AWS X-Ray, Amazon Managed Grafana, and Amazon Managed Service for Prometheus, to provide excellent observability in its environment. It can work in a hybrid solution supporting on-site collectors from Amazon or OpenTelemetry.

CloudWatch comprises several tools, including CloudWatch Application Insights, CloudWatch Synthetics, CloudWatch Network Monitor, CloudWatch Observability Access Manager, CloudWatch RUM, CloudWatch Evidently, CloudWatch Container Insights, CloudWatch Logs, CloudWatch Logs Anomaly Detection, Container Insights, Lambda Insights, Internet Monitor, and CloudWatch Natural Language Query Generation (in preview with GA in early 2024). Additionally, Amazon

CloudWatch offers metrics and alarms with dynamic dashboards as foundational capabilities.

Application Signals, which can be used to instrument applications and track their performance and health, includes synthetics, RUM, service map, and tracing. Like Application Signals, Amazon Logs Anomaly Detection is powered by AI/ML, providing an automated logs analytics feature with natural language query generations. CloudWatch offers the Embedded Metric Format (EMF), which enables customers to enrich metrics and logs with additional context.

AWS provides observability tools, including monitoring, logging, alerting, and dashboards, for Amazon Elastic Kubernetes Service (Amazon EKS) projects. This includes Amazon Managed Service for Prometheus, Amazon Managed Grafana, and AWS Distro for OpenTelemetry. AWS provides Terraform modules that configure observability with these services, called AWS Observability

Amazon does well with edge monitoring using synthetics and CloudWatch agents. Adding AWS Systems Manager and AWS Outposts provides more capabilities for managing edge computing infrastructure, and using FreeRTOS, a real-time operating system with built-in libraries, can create a secure connection with AWS services. Thus, AWS can provide exceptional edge observability capabilities using CloudWatch alone or with add-ons. Finding ghost changes is an emerging feature Amazon has not invested in.

Strengths

CloudWatch scored particularly well in this year's business criteria. The deployment is essentially automatic, with some work for on-site data collection and other clouds. The agility of the solution is strong, with a large number of modules available to meet most needs. However, the downside to this is increased complexity. Security is enhanced by the availability of security information and event management (SIEM) and security orchestration, automation, and response (SOAR) for CloudWatch.

The Amazon ecosystem is extensive, with options for training, professional services, community interaction, partner programs, and more. The online documentation is also extensive, though it is easy to go in circles due to frequent cross-linking of topics. These factors contribute to a high score for the ecosystem business criterion.

Challenges

If there is a weakness in the Amazon approach, it is its concentration on AWS, with any other cloud, public or private, left to the customer to deploy using Amazon or OpenTelemetry collectors. AWS has announced pending improvements in multicloud support. Also, the modular nature of the offering—as outlined above—can be confusing for prospective customers, but it also allows Amazon to improve CloudWatch quickly. As with most in the industry, Amazon has little support for ghost changes.

Purchase Considerations

CloudWatch produces the best results when operating within the AWS cloud. Within that environment, additional features such as SIEM, SOAR, and world-class

support are available. A hybrid environment with Amazon or OpenTelemetry collectors can be a bit more difficult due to the need for open source skills and the sheer number of options, more so than other SaaS offerings. Amazon does, however, offer an agentless element of the Amazon Managed Service for the Prometheus collector, which eliminates the need for any additional skills or instrumentation with a two-to-three click setup similar to native solutions.

If AWS is the primary public cloud used, then CloudWatch should be considered. Those with multiple public and private clouds should investigate other solutions and AWS. CloudWatch is a pay-as-you-go service that measures usage and bills monthly. The price of some features is tiered based on volume, but CloudWatch offers a free tier for all features. With the AWS pricing calculator, cost estimates can be built for self-serve and customized versions to monitor workloads and use cases.

Amazon CloudWatch is suitable for any size enterprise that primarily uses AWS. Support for hybrid environments is possible. Those with open source skills will be more successful operating CloudWatch in non-AWS environments.

Radar Chart Overview

Amazon is considered a Feature Play because of its primary support for AWS. Though CloudWatch is being updated often, it is considered a mature product. It falls within the Challenger group on our chart but is considered an Outperformer due to the rate of change in the solution—improvements are made as quickly as they are identified. Updates can be as frequent as daily.

BMC: BMC Helix IT Operations Management (ITOM) Suite

Solution Overview

BMC is known for its large platform portfolio covering everything from mainframes to cloud computing. Its observability solution is the BMC Helix IT Operations Management (Helix ITOM) suite, which uses ML to analyze large volumes of data (events, metrics, traces, logs, topology, ITSM data such as incidents, and more) to identify patterns and anomalies, predict future problems, and recommend automated solutions.

Helix ITOM scores well as a cloud observability offering on a number of key features. Its strong dashboards are easy to create, modify, and customize. The multicloud functionality covers the major public clouds and allows private cloud participation. Its predictive analysis capabilities are excellent as well, with 12-hour service forecasts, saturation forecasting up to 90 days out, and what-if simulation for several months when there is two to five years of data available.

The solution also does well in several business criteria. Deployment is simple in a SaaS environment, while on-site deployment uses containers and support from a deployment manager. These tools ease the process of adopting Helix ITOM. Ease of use is also strong with easy-to-customize dashboards and reports. The solution's agility is good, enhanced by the low-code/no-code capabilities and out-of-the-box integrations. Additionally, the BMC ecosystem is extensive and provides better-than-average support for users

In the emerging area of edge observability, BMC Helix Edge allows anomaly detection, predictive maintenance, asset inventory, and asset lifecycle management. Coupling these capabilities with Helix ITOM's synthetics makes a complete edge observability solution possible.

The need to find ghost changes is becoming more important as the complexity of applications grows. BMC does not have a purpose-built solution for finding unplanned changes in software and configurations; however, it can detect infrastructure changes and highlight anomalies that may have a source in a ghost change. BMC can use predictive, causal, and generative AI to find changes and remediate them.

Strengths

Helix ITOM is a strong product with excellent dashboards, multicloud abilities, and good predictive analytics if sufficient data is available. It is easy to deploy and use, with unexpected agility and flexibility. The BMC ecosystem is another area of strength. The ability to build an edge observability solution is surprising, but the cost of having to use another package may temper that facility.

Challenges

The lack of the built-in synthetics transaction support offered by the other leading observability tools (Helix ITOM relies on Catchpoint as a third-party solution with additional costs) is a challenge. Edge observability is possible but also comes with additional cost. Security enhancements that include SIEM and SOAR can be integrated seamlessly but are separate SKUs.

There are a few other weaknesses as well. The use of OpenTelemetry is supported, but it must be configured before it can be used. Moreover, BMC does not contribute to the Cloud-Native Computing Foundation (CNCF) OpenTelemetry project; however, the current roadmap includes contributions to the standard.

Purchase Considerations

Unless an enterprise is already using BMC, it would not be on most companies' shortlist for observability tools—but the offering is worth considering, especially for large enterprises and service providers, particularly if they already own BMC products. Enterprises and service providers benefit most from BMC's offerings due to the scale of BMC and the scope of their solutions. Small businesses are not a target market for BMC.

Licensing uses tiered suite pricing by asset with subscriptions. Adding additional products can complicate pricing.

Radar Chart Overview

The target market for BMC Helix ITOM is enterprises and service providers, and the solution is well established. It is, therefore, within the Maturity half of the Radar. It competes in functionality and ease of use with several other platform players. Although BMC is not well known for cloud observability, it has leadership qualities that larger enterprises should examine. It moves forward at a moderate pace to add product functionality and features. Though BMC is rarely considered a bleeding-edge company, its generative AI capabilities put it in the forefront, at least in this area.

Broadcom: AIOps and Observability

Solution Overview

Broadcom AIOps and Observability is a suite of products that includes analytics, automation, and collaboration capabilities, a topological model, and integrations with monitoring technologies across applications, middleware, and infrastructure. There is full support for OpenTelemetry, but Broadcom is not a contributor to the initiative.

Looking at key features, the solution has average scores for reporting and dashboards, pushing and tagging data, and LLM support. Broadcom's DX Dashboards are based on Grafana, with built-in connectors to the Broadcom data lake. Dashboards are populated when agent data becomes available, and many out-of-the-box templates are available. REST API integrations support pushing and tagging data, and SIEM logs can be ingested. Current LLM support allows NLP alarm correlation and clustering models using time, text, topology, and services. Other LLM improvements are on the vendor's 2024 roadmap, including correlated alarms and metrics for impact summary at the service and monitored entity level, contextual product help, and heuristics-based "similar" alarm summaries about incidents, with notes and the ability to make recommendations.

Broadcom has above-average scores for user interaction monitoring, multicloud functionality, and predictive analysis. User interaction monitoring comes from OpenTelemetry, on-premises RUM for HTTP, and mobile requests with full session replay and funnel analysis. Multicloud functionality allows pushing and tagging data effectively. Synthetic transaction monitoring covers everything from mobile to mainframe. Ninety worldwide synthetic locations are available, as is on-site support for walled gardens. Multicloud functionality includes all major public cloud providers (in multiple regions) and can provide perspectives for the environments in a single interface.

In terms of emerging technologies, Broadcom can create synthetic transactions to monitor edge resources but lacks observability computing at the edge. The breadth of its synthetic transactions gives it a good rating for edge observability. Most vendors find detecting ghost changes difficult, but Broadcom can see some unplanned infrastructure changes. Improved detection of software and configuration changes is on the roadmap.

Looking next at business criteria, Broadcom has average scores for ease of deployment, ease of use, and security. The solution is containerized and supports deployments over Kubernetes or OpenShift. It uses Helm chart-based installation for ease of deployment. In the near future, Broadcom will use eBPF as its universal monitoring agent (UMA). Its application command center (ACC) combines agent bundle management, agent lifecycle management, and automated deployment of agents. ACC also acts as a self-service portal for agent downloads and deployment guidance, including versioning, audit, and rollback scenarios. UMA is integrated with ACC, allowing the containerized zero-touch agent to discover and instrument cloud and container components automatically. There are two admin consoles for solutions with both on-site and SaaS usage, but one interface for users. The API framework is well-documented and supports ingestion and query

use cases. Security includes standard features like RBAC and SSO, along with support for SOC2.

Broadcom has above-average ratings in agility, ecosystem, and cost. Agility, especially, within an all-Broadcom environment, enables observability from mainframes to mobile devices. Customization for developers is constrained by RBAC access to APIs. Authentication and authorization of encrypted tokens with time to live and on-demand reset options are guardrails. The Broadcom ecosystem is what would be expected from a large platform-focused vendor. It includes customer and partner-specific “lunch and learn” sessions, a dedicated partner portal, certifications, user communities, regular product team access, and monthly events to share solution updates and gather feedback.

Strengths

Broadcom can monitor any object from a mainframe to a mobile device. RUM is available in any cloud and on-site. Predictive analysis can be seasonal, limited only by the amount of data available. Agility is better than average with the use of low-code/no-code tools and developer support anywhere in the enterprise. The support ecosystem is extensive.

Challenges

The requirement for two admin consoles, one for on-premises and another for SaaS, could be problematic, but the user side has a single interface for both SaaS and on-site. The use case for both installations is likely limited to service providers—the SaaS solution with on-site agents is more common.

Purchase Considerations

The solution is available as a Broadcom-hosted SaaS service (DX SaaS) over GKE in North America and Europe. Broadcom has a cloud-native container-based version for on-premises self-managed deployments.

Broadcom offers a large platform, as it has acquired several companies over the last few years. It's not well-known for cloud observability and so isn't usually on many short lists. Organizations already invested in Broadcom products should look at the solution, as it may seamlessly integrate with existing products in the Broadcom portfolio.

Licensing is by normalized device metrics for consumption-based licensing, subscription-based licensing, and licensing by customer segments determined by size, geo-location, and reselling models. Dashboards can assist in containing costs, correlating the devices used for charging the actual data ingestion in near real-time.

Broadcom serves organizations of all sizes, including service providers. It can handle multiple cloud environments, which can be important when more than one public cloud vendor is in use or for private clouds with secure information.

Radar Chart Overview

Broadcom is a mature platform that is moving forward steadily. Broadcom is a Challenger due to average scores across most of the decision criteria we evaluated, but its offering is compelling and worthy of consideration, especially for

enterprises already invested in Broadcom products.

Chronosphere

Solution Overview

Chronosphere is a SaaS observability tool based on proprietary software with the ability to ingest data from both open source and proprietary formats.

Chronosphere can observe workloads running in public and private clouds.

Chronosphere features Lens, a service-oriented group of resources such as dashboards and monitors, with links to home pages where users can find dedicated dashboards (many are prebuilt). Data can be analyzed using dashboards (no-code), investigated with queries (low-code), and monitored to generate notifications and alerts. Data is ingested via a proprietary Chronosphere collector, the OpenTelemetry collector, or the open source Fluent Bit collector.

Ingesting MELT can increase data and storage costs. Chronosphere uses several methods to control that data. It can profile and analyze metrics for their usage and cost, create drop rules to drop incoming metrics based on labels (tags), shape data with quotas, persist metrics reduced performance needs, and create rules to control costs and maximize the usefulness of trace data.

However, Chronosphere lags behind in LLM support and predictive analytics. The company is actively researching this area, but nothing is in production or on a definitive roadmap. Prediction of future states is limited, but by leveraging PromQL, some predictive work can be done within the limits of that open source tool.

The solution is capable of edge observability via OpenTelemetry and Calyptia, which Chronosphere acquired in 2024. Calyptia is built on the CNCF open source projects Fluent Bit and Fluentd. Ingestion and computing analytics can therefore be done at the edge. Identification of ghost changes is not a real feature of Chronosphere, but with careful configuration, the discovery tool can identify changes in infrastructure. Chronosphere can also integrate with other DevOps tools (CI/CD, feature flags, and so forth) to identify changes in infrastructure. Proper configuration of Lens as a service discovery pipeline can also show additional components as they come online.

Chronosphere is strong in the business criteria of ease of deployment, ease of use, and agility. Deployment for SaaS only is simple, but multicloud and on-site collection of data requires skill with open source technologies. Ease of use is good, with no-code tools for dashboard creation, but low-code and pro-code skills are required for analyzing metrics, creating notifications, and alerting.

The standout area for Chronosphere is cost-effectiveness. The Chronosphere dashboard allows tracking telemetry usage against licensing quotas. Aggregations—and tools to support them—enable persisted writes to the database and persisted cardinality, which results in lower storage costs. Capacity limits indicate the maximum license for metric data, while a dashboard for tracing consumption helps control persisted trace data.

Strengths

Overall, Chronosphere is a capable observability tool with superior cost-management abilities for administrators and developers. The ability to aggregate and filter data so that only needed data persists lowers storage costs and improves performance. Analysis tools for traces, events, logs, and metrics assist in decision-making. There is superior support for data gathering from the major public clouds and private clouds. Dashboards, user interaction performance (RUM) monitoring, and pushing and tagging data whether using OpenTelemetry or API integration receive an average score.

Edge computing is an emerging technology that Chronosphere is capable of delivering using recently acquired technologies from Calyptia.

The ecosystem for Chronosphere includes documentation, training, a recently initiated partner program, and community involvement via forums.

Challenges

Support for LLMs is absent, though Chronosphere is researching this area to determine customer needs. Another absent key feature is predictive analysis. Chronosphere is unable to predict the future state of a metric or groups of metrics via linear regression or other algorithms.

Purchase Considerations

Chronosphere can work with companies of any size with dedicated/active observability teams looking to control their observability budget. Extremely innovative enterprises with strong skills in open source software and a strong software development team should consider Chronosphere. The company's engagement with customers is strong, and users can participate in the future growth of the solution. The roadmap indicates there will be significant changes over the next 18 months. Small teams may benefit by engaging now and reaping the rewards as the product develops.

Radar Chart Overview

Chronosphere is a new and innovative vendor, placing it on the Feature Play side of the Radar. It did not score as well as other vendors in the decision criteria we evaluated and is positioned in the Entrant ring. Its cost optimization feature is notable in that it provides methods to persist only the data needed via filtering and transformation.

Cisco: Full Stack Observability

Solution Overview

Cisco, after acquiring AppDynamics and ThousandEyes, has now completely integrated their technologies into Cisco Full Stack Observability (FSO), which focuses on bringing together data from anywhere in the enterprise.

Cisco garners a superior score on almost all of the key features, notably data-driven visualization, synthetics, and RUM, pushing and tagging data, and performing predictive analysis. LLM support received an average score, but its use of LLMs is moving in the right direction, with model observability to monitor models and APIs to observe deployed models, monitor their performance, and

extract key insights such as costs incurred.

With a hybrid model, Cisco can build edge observability, but design and execution may require manual steps or professional services. As with most vendors, Cisco fares poorly with ghost changes, though service topology maps and infrastructure are updated when changes take place.

Looking at the business criteria, standout areas with superior ratings include ease of deployment, ease of use, agility, and security. Deployment for SaaS is easy in principle because all Cisco FSO solutions are SaaS. No deployment is necessary for initial access. However, the complexity of the environment can tangle efforts, particularly for on-site and hybrid SaaS deployment. To deploy collectors on your cloud-based Kubernetes cluster, you must download binaries and follow deployment instructions.

Platform monitoring provides visibility into the runtime status of the Cisco Observability platform. Cisco continues the superior rating for ease of use with a consistent user interface and a mostly no-code or low-code customization environment. Agility is enhanced with strong workflow flexibility. The solution also supports dashboards, microsites for application experiences, and a customer-centric governance model.

Cisco has an average score for its ecosystem. Documentation for Cisco FSO is located on the AppDynamics website (not on the Cisco website), making it difficult to find, but all other ecosystem requirements are better than average.

Cisco FSO supports a strong set of security features, including SSO, RBAC, GDPR, data encrypted at rest, no PII by default, and PCI and PII masking. Additionally, the Cisco Secure Application is embedded, resulting in a superior mark for this business criteria.

Strengths

Cisco has superior scores in most key features (dashboard, user interaction, multicloud support, pushing/tagging data, and predictive analysis). The ability to create an edge observability solution places the company ahead of the curve. Strong business criteria include ease of deployment, though with less strength for hybrid deployments. The solution is easy to use with a consistent look and feel in all areas. The use of low-code and no-code tools supports the superior ranking for agility. Security is another strong area, with Cisco Secure Application as part of the solution.

Challenges

Cisco is moving in a positive direction with LLMs, but support at this time is only average compared to the market, with simple user interaction via bots and connections to external LLMs. The identification of ghost changes remains an opportunity for Cisco, as with most other vendors. Documentation is found via the AppDynamics website and can't be found on the Cisco site.

Purchase Considerations

Cisco FSO belongs on the shortlist of any organization looking into observability. When used entirely as a SaaS application, it is a leader in almost every category. In

a hybrid configuration, it is still very good, but additional work is necessary to configure collectors and agents for edge and on-site use.

Licensing is by tiers, with Premier containing the entire FSO toolkit, which includes hybrid application monitoring, cloud-native application monitoring, application security, customer digital experience monitoring, application dependency monitoring, hybrid cost optimization, and application resource optimization. For enterprise-level users, this is the most likely package. The other tiers, Essentials and Advantage, have fewer packages and should be investigated for those who need a smaller footprint.

Cisco targets enterprise markets first but actively sells to SMBs and service providers. Cost is a consideration for any use case. Cisco's FSO Hybrid Cost Optimization tool leverages AppDynamics and its Cost Insights to suggest infrastructure changes to optimize performance while minimizing cost.

Radar Chart Overview

Cisco is on the Platform Play side of the Radar, as it contains many capabilities and products that work together. Due to its strong feature set, it continues to be a Leader in the observability space. In this year's evaluation, it is positioned in the Innovation half, as it continues to innovate steadily, adding new and interesting features regularly.

CloudFabrix: OneNetwork Observability

Solution Overview

CloudFabrix is an important player in the AIOps vendor space, which is now expanding into cloud observability. Much of the CloudFabrix OneNetwork Observability offering is built on its Robotic Data Automation (RDA) Fabric (RDAF), which creates rich pipelines anywhere in the infrastructure. Open source tooling has been added to fill in the areas where the AIOps offering has holes for cloud observability. In addition, OpenTelemetry MELT can be consumed.

CloudFabrix offers several key features with a superior rating. RDAF bolsters the CloudFabrix LLM, called Macaw, which enables conversational queries, AI-powered dashboards, dataset analytics, and AI for intent-driven automation. The ability to work with all major cloud vendors as well as private clouds is also compelling. CloudFabrix also gets high ratings for multicloud functionality, pushing and tagging data, and predictive analytics. Prediction of future problems, where the forecast is only limited by the amount of historical data available, is another strong area for CloudFabrix.

Dashboards and reports provide summaries where needed and are able to drill down as far as necessary. A FinOps module is also available.

CloudFabrix is the only vendor to receive a superior rating for edge observability, chiefly due to its use of RDA Edge Nodes to collect and compute data at the enterprise edge before using pipeline technology to forward the results. However, while it may be possible to have the Macaw LLM look for ghost changes in the environment, the results are not certain. And ghost changes can't otherwise be found by CloudFabrix.

Deploying CloudFabrix for SaaS only in a public cloud environment is easy. Setting up RDA in a low-code environment is also relatively simple. The creation of a hybrid environment with OpenTelemetry or other open source tooling can be more challenging—this requires command language instructions for configuration, so deployment is considered average.

Ease of use is superior once deployment is complete. The agility ranking of CloudFabrix is a mixed bag. RDA and deployment of CloudFabrix tools are relatively easy, but if external monitoring data uses open source tooling, deployers will require skills with open source code.

The CloudFabrix ecosystem has an average score but is missing online training and certifications. Documentation may not be as current as the products and marketing. Security is average, with support for both SSO and RBAC. Cost is also average, with licensing by asset and costs for storage of data on a sliding scale based on volume.

Strengths

The Macaw LLM is a specific strength, as is the ability to work with all major public and private cloud vendors. Multicloud functionality, pushing and tagging data, and predictive analytics are also strong areas for CloudFabrix.

Challenges

Deployment into a hybrid environment may require specific technical skills, particularly for the open source capabilities needed to feed metrics, logs, and other data. In addition, CloudFabrix is not strong in the ability to find ghost changes.

Purchase Considerations

CloudFabrix has a well-established reputation in AIOps, and the company is now adding observability. Those already using CloudFabrix's AIOps solution should look at the observability tooling because many components are shared. Observability does use more open source software, which may deter some organizations. As the current solution is CloudFabrix's initial observability product, substantial improvements can be expected next year.

CloudFabrix targets large organizations and service providers. RDAF and the data pipelines therein allow the ingestion of data from any location within the enterprise. CloudFabrix is not recommended for SMBs—its marketing concentrates on large enterprises and service providers.

Radar Chart Overview

CloudFabrix is positioned in the Maturity/Platform Play quadrant. It is a Challenger due to its solid scores across most of the decision criteria we evaluated. The vendor is a Fast Mover, given its introduction of an observability tool since the last Radar.

Datadog

Solution Overview

Datadog is a SaaS platform that integrates and automates infrastructure

monitoring, APM, log management, RUM, and other capabilities. The company is known for its monitoring and observability modules, which allow enterprises to choose the tools they need to improve IT operations. Datadog offers a number of modules that covers infrastructure, applications, security, and logs, with multiple module options in each area.

Datadog has a superior rating in all of the key features except LLM support, which is rated as average. Datadog uses Bits AI for interactive querying of data and AI Firewall to inspect incoming and outgoing queries to external LLMs.

Dashboards and reporting, user interaction performance, pushing and tagging data, and predictive analysis are all areas where Datadog scores are better than average. Dashboards are no-code or low-code. User interaction performance handles RUM and traces from OpenTelemetry. Pushing and tagging ranges from extremely easy to a bit tedious, and Datadog can forecast days, weeks, or months into the future, depending on the amount of historical data available.

For the emerging features in this Radar, edge observability is poor, with only synthetic transactions available and no edge computing power. There is no direct support for ghost changes, though infrastructure change detection is possible using pro-code.

Datadog does a superior job in five of the six areas of business criteria. Ease of deployment is very straightforward since Datadog is a SaaS system, though setup can take a while if multiple modules are deployed. The system is easy to use, and despite the large number of disparate modules, the UI is consistent and easy to navigate. The Datadog ecosystem is comprehensive and includes training, certifications, community support, professional services, and a partner program.

The agility of the solution is superior, with extensive integration capabilities and low impact on developers. Third-party open source tools are used for Kubernetes, OpenTelemetry, and applications built using the Go language. Datadog Vector is an open source product developed for building observability pipelines.

Cost control is average, but each of the more than 20 modules has a unique cost model. Some use device counts, others have consumption models, while at least one has a cost structure that depends on the public cloud used. A free tier allows enterprises to test Datadog features across modules.

Strengths

Datadog is comprehensive, handling all parts of IT operations, including support for developers. Low-code and no-code tools are used extensively, with the occasional pro-code required for some open source tools. The solution is easy to deploy and use with the flexibility to handle any size organization. The vendor's cautious approach to generative AI is a plus as this technology finds its level in the next few years.

Challenges

This is a capable platform, but the number of modules can make cost control difficult. Moreover, while users can use the modules immediately, the extensive use of multiple modules may require professional services.

Purchase Considerations

Datadog is a significant player in the cloud observability space and is often on the shortlist of companies looking for solutions. Determining which components are critical to the organization and creating a solution may require professional services. Large companies can negotiate with Datadog on licensing.

Datadog is used by organizations of all sizes and across various industries. Several verticals are supported, including financial services, manufacturing, healthcare, e-commerce, government, education, and gaming. Common use cases are extensive, like all things Datadog. A partial list includes cloud development and deployment, security analytics, IoT monitoring, and log analysis.

Radar Chart Overview

Datadog is an extensive platform with mature features, placing it in the Maturity/Platform Play quadrant. Its change rate is more measured than others in the market, giving it a Forward Mover designation.

Dynatrace

Solution Overview

Dynatrace is a SaaS platform with AI and automation built in. Dynatrace is described as an all-in-one observability, security, analytics, and automation platform for cloud-native, hybrid, and multicloud environments.

The Dynatrace solution has exceptional ratings in two key features: dashboards and reports and user interaction performance. Dashboards can be generated in a low-code/no-code environment or using generative AI. User interaction performance is an area in which Dynatrace has long specialized, using its OneAgent technology to support RUM, synthetics, session replay, and traces from OpenTelemetry. It fully supports OpenTelemetry and is a major contributor to the open source project.

Multicloud support and LLM support are rated as superior. Dynatrace can be used in any public or private cloud, though collectors are necessary for on-site deployment. Dynatrace offers LLM support with Davis AI, Grail, and the DQL query language. The ability to push and tag data is also superior. The OneAgent technology allows easy tagging, and data can be pushed almost anywhere via APIs.

Dynatrace received an exceptional score in predictive analysis. Its Davis AI prediction algorithm automatically analyzes training datasets; identifies seasonality, noise, and trend features; and uses those to select the best-fit prediction model for the data. The Dynatrace prediction algorithm can be used on any data the user specifies to provide forecasts for a time period at least three times longer than the typical prediction horizon.

Dynatrace offers a formal edge observability solution using Red Hat servers and agents on the edge. Unplanned and unapproved ghost changes cannot be seen directly; however, Smartscape can be used to see topological changes to applications, processes, hosts, and data centers. So it doesn't find actual changes to code, configurations, or parameters, only the possible result of a change.

Dynatrace has a superior rating on all business criteria except ease of use, which is considered average and is now on par with other vendors.

Ease of deployment garners a superior score. Dynatrace has improved in this area with topology awareness, zero-configuration, auto-discovery, configuration-as-code, and dynamic code injection. Dynatrace Hub is a feature enhancement, providing a central place to explore and activate all capabilities, thus improving ease of use to average.

Agility, the ecosystem, security, and cost all receive a superior rating. Agility is supported by a low-code/no-code approach with pro-code as a fallback to create notebooks, dashboards, workflows, and Dynatrace Apps. An enterprise can adapt Dynatrace to the way it needs to work. The Dynatrace supports an active online community, and documentation is online. There are also clinics, forums, professional services, a strong partnership program, and Dynatrace University for training.

Strengths

Dynatrace is strong in almost all technical areas. Dashboards, RUM, tracing, multicloud functions, LLMs, tagging, and predictive analysis are all better than average in the cloud observability world. Deployment ease remains a strength, and ease of use has improved, with more improvements in the 2024 roadmap.

Challenges

The platform has gained new capabilities quickly, including more functionality in Grail, Davis AI, and continuous updates to OneAgent, creating the need for other improvements in ease of use. Dynatrace could consider looking into ghost change detection to improve a good observability solution.

Purchase Considerations

Licensing is via a Dynatrace Platform Subscription (DPS) and an account management portal. There are no monthly minimums, high watermark charges, or per-user fees. No penalties are charged for usage that exceeds the annual commitment, and consumption-based pricing is available. The flexibility and control for licensing and cost are superior.

Dynatrace is a major player in cloud observability. In the past, the technical complexity of its solution limited quick adoption. The latest updates address ease of use and training, allowing less technical enterprises to place Dynatrace on their shortlist of solutions to review for quick improvement to their cloud observability footprint.

Marketing from Dynatrace continues to target the largest enterprises. Vertical industries supported include financial services, e-commerce, government, travel and transportation, education, and more. Dynatrace has more improvements on the 2024 roadmap, including AI analytics enhancements, a new telemetry pipeline (OpenPipeline), security posture management, and capabilities such as live debugging for developers.

Radar Chart Overview

Dynatrace, with its deep feature set, continues to be a Leader This year, it is positioned in the Innovation/Platform Play quadrant due to its focus on new features and product changes. As it is a long-time player in this category, the maturity of its features is assumed.

Elastic: Elastic Observability

Solution Overview

Elastic is an open source and proprietary observability solution with both managed and self-managed offerings. The solution contains APM, logs, metrics, and synthetic monitoring. Elastic Security is part of the Elastic portfolio but is not included in Elastic Observability.

After ingesting logs, infrastructure metrics, application traces, user experience data, and synthetics into Elasticsearch for possible processing and enhancement, Elastic Observability unifies them and does universal profiling. The user interface offers built-in visualizations, service maps, and distributed tracing waterfalls, as well as ML features such as anomaly detection, log pattern analysis, and correlations-based root cause analysis, and a chat-based AI assistant for interactive ad hoc exploration. Visualization and adding alerts can also be done in Kibana, a dashboarding tool that is part of the free Open ELK stack.

Dashboards built with Kibana are low-code, but not all dashboards can be customized using low-code tools and may require pro-code skills. User interaction performance is also average with RUM and synthetic support.

Elastic's Uptime solution is a legacy product that has been replaced by Synthetics; however, it continues to be supported (but not developed). Uptime enables viewing result data from lightweight monitors running through Heartbeat, an open source monitor. Uptime uses Elastic Agent to check the status of services and applications. For browser-based monitoring, Elastic suggests using the Synthetics app instead. Both may be appropriate, depending on the needs of the enterprise.

Also receiving an average assessment is Elastic's ability to tag and push data. Tags are defined in Kibana. Pushing information is handled via API integration. Multicloud functionality is available for public and private clouds, resulting in a superior score for that feature.

Elastic AI Assistant can request, analyze, and visualize data, and provides LLM capabilities via integration with an enterprise LLM provider. Data sent to the AI Assistant is not anonymized, and overall, LLM support is considered to be limited. The ability to predict or forecast data from metrics or other time-series data is limited. Enhanced predictive analysis capabilities are under technical review with expected general availability in early 2024.

Edge observability is possible but would require a design for edge computing and deployment by the enterprise. Identification of ghost changes is poor, but with pro-code, infrastructure changes can be detected.

Business criteria are all average. The ease of use within Kibana, the user-facing portion of Elastic, is average. Some customizations are low-code, while others

require more pro-code skills. The agility of the solution is also adequate.

Strengths

Elastic Observability is, on the whole, a capable observability solution. Other than multicloud functionality, there are no features that stand out, however. Adding Elastic Search and Elastic Security to the observability tools may be the ideal solution from Elastic.

Challenges

Though capable in all areas, deployment for on-site and general ease of use need improvement. Kibana's interface is not that easy to use, while deployment requires more pro-code capabilities that many shops would be comfortable with.

Purchase Considerations

SaaS deployment is straightforward using Elastic Cloud. On-site deployment can be complicated due to the number of moving pieces and the level of pro-code necessary, though Elastic provides guidelines and additional documentation to help. Professional services are also available.

The Elastic Observability product is based on many open source tools. Pro-code skills are necessary for some functions, such as customizing ingestions, and these skills, which may be necessary to get maximum usage of the offering, may not be present in all organizations. Service-level objectives (SLO) are available and represent a feature not offered by many observability vendors.

The basic security functions for SSO, RBAC, and encryption meet industry standards. An additional security module is available to unify SIEM, endpoint security, and cloud security.

Elastic Observability is also competent in terms of cost. Licensing tiers range from Standard to Enterprise, with a free tier also available. A pricing calculator is available to assist customers in planning and forecasting costs. Some features are volume-based, and the calculator helps with the effort of cost control. Elastic Observability subscriptions on AWS GovCloud (US) are only available annually. Elastic provides support for all tiers of Elastic licensing.

Open source experience is essential to obtain the most from Elastic Observability. Those looking for an open source solution should have Elastic on the shortlist. The free tier can be used to create a proof of concept, with the suitability of the other tiers aligned to the size of the enterprise. Consider adding Elasticsearch and Elastic Security to create a complete deployment.

Elastic Observability is aimed at organizations of any size. Any organization looking to base its IT operations on open source software is a prime candidate for Elastic Observability.

Radar Chart Overview

Elastic Observability is positioned in the Maturity/Feature Play quadrant. Within this area are open source solutions and solutions primarily for a single public cloud. Elastic is near the border between the Entrant and Challenger rings, with expectations that, as an Outperformer, it will move forward quickly due to its rapid

release schedule and the significant contributions from its user community.

Grafana Labs: Grafana Cloud

Solution Overview

Grafana Cloud is a fully managed OpenSaaS observability platform offered by Grafana Labs. It provides a solution for observing metrics, logs, and traces, with options for synthetic monitoring and ML capabilities, and includes dashboards. For this evaluation, Kubernetes monitoring, application observability, and frontend observability define Grafana Cloud.

Grafana is the reporting and dashboard backbone for many vendors. It provides an extensive collection of templates to view data from any of the open source components of Grafana Cloud and other data sources. The Grafana community also contributes dashboards, making it a superior performer. Also superior is predictive analysis via Grafana ML. Grafana ML can use up to 50,000 samples per series and provides a number of configurations for predicting the future performance of time-series data. Other key features are average. User interaction performance uses OpenTelemetry ingest traces.

Multicloud functionality includes all major clouds and, with the help of the self-managed version of Grafana Cloud, private clouds and walled gardens. LLM support using generative AI in dashboards is currently in public preview. Pushing and tagging data is accomplished using a variety of open source tools. Some tools offer low-code features, but pro-code skills are necessary for some API integrations.

Edge observability is not specifically a feature, but by using synthetics and the self-managed offering, an enterprise may be able to create an edge solution. A poor rating in this area is common in this space. Using pro-code to create a solution for identifying ghost infrastructure changes may be possible.

Other than the superior ecosystem of Grafana, all other business criteria are average. Deployment is simple for the SaaS version of Grafana Cloud. The self-managed version can be complicated due to the number of moving pieces: Loki for logs, Grafana for dashboards and visualization, Tempo for traces, and Mimir for metrics. In some cases, major releases may add new features and also break other parts of the deployment. Grafana publishes changes and tells how to fix anything that breaks due to the update. Grafana releases updates up to 50 times per year.

Ease of use for visualization does well because of the low-code environment, but some dashboards have to be built from scratch or customized from one of the provided templates. This may be a time-consuming process. Application observability Kubernetes, front-end monitoring, and infrastructure integration all come with prebuilt out-of-the-box dashboards. Security includes SSO and RBAC.

Strengths

Grafana dashboards are a standard used by other vendors. Predictive analytics is also a strength. The number of data points for a forecast is limited, but the timeline can be as long as desired. The ecosystem for Grafana reflects its open source roots and is extensive, although certifications are not possible.

Challenges

Grafana Cloud is based on open source components. Skills using open source tooling and pro-code development are necessary to obtain the best from the solution.

Purchase Considerations

Grafana Cloud licensing has a free option and two additional tiers. One is a supported pay-as-you-go option. The other is a monthly subscription at higher levels of support. There are additional charges for metrics, logs, traces, visualization, profiles, and Kubernetes based on consumption volume. Grafana Enterprise is a self-managed option with custom pricing.

A shop with open source experience should have Grafana on their shortlist of vendors. Successful use of the free version may be a gateway to a supported version of Grafana.

Marketing for Grafana Cloud is to any size institution. If the enterprise is looking for an open source solution, Grafana should be considered.

Radar Chart Overview

Grafana Cloud is positioned in the Maturity/Feature Play quadrant. Within this area are other open source solutions and single public cloud providers. Grafana is a Challenger and Outperformer in the marketplace, with as many as fifty updates per year.

Honeycomb

Solution Overview

Honeycomb has a DevOps and engineering team-focused observability solution that uses its own code and OpenTelemetry. Honeycomb supports and contributes to OpenTelemetry. It supports eBPF to generate telemetry outside of the application space using kernel probes for detection.

Honeycomb's innovative BubbleUp feature ranks as superior within the cloud observability space. Dashboards begin with an initial query to their multidimensional datastore. This is a notable feature and is accessed via low-code queries. BubbleUp visualizes data points from any query result grouping and runs automatically on failed service level indicator (SLI)-tied events in the alerting system, which compares them to the remaining data. Values that "bubble up" can be isolated and investigated as to the root cause. User interaction performance has a solid interface with support for traces but not synthetics.

Honeycomb uses OpenAI's API for its Query Assistant to create a working generative AI visualization of any query data. Observability for posting and retrieving traces from LLMs is supported—Honeycomb allows the customer to see what is sent to OpenAI, including the response. LLM outputs are nondeterministic; Honeycomb can analyze which outputs fail or contain failure patterns. The query assistant sends the natural language query to OpenAI with the names of fields in the dataset schema, but Honeycomb does not send any identifying information or values in source data to OpenAI. Tags, including deployment markers, can be added manually using low-code or pro-code with the API, and data can also be

pushed using the API.

Honeycomb supports the definition of event-based SLOs and can make predictions for the SLOs. Despite this, the solution offers less-than-average performance for predictive analytics and does not support the prediction of metric data.

Honeycomb does very well with edge observability, with full support for edge collectors and computing power on the edge. Ghost changes are not explicitly supported, but service maps go back sixty days and thus reveal system changes and migration progress across that timeline. The company also supports audit logs, allowing admins to track changes in configurations.

Deployment of the SaaS is on AWS in North America or a GDPR-compliant instance in Europe, contributing to a below-average ranking. All other deployment options are with OpenTelemetry collectors managed by Open Agent Management Protocol (OpAMP), a part of OpenTelemetry, and in their Kubernetes instrumentation, by Helm. Overall, Honeycomb's deployment rating is average.

Ease of use is superior due to the BubbleUp feature. Honeycomb has yet to achieve the agility and flexibility of other solutions but is still capable due to low-code capabilities in most areas and no-code for Kubernetes monitoring. Honeycomb has no partner program, but documentation and training are available, with no certification. Security follows the market standard of SSO, RBAC, and encryption. Honeycomb has a simple cost model with a free licensing tier. There are a few consumption-based areas, such as events, triggers, and SLOs, and data retention is sixty days for all licenses, with longer terms possible at the enterprise level.

Strengths

Honeycomb's BubbleUp feature is its strongest selling point. Its LLM use is notable in this early phase of generative AI and provides an easy-to-use (after initial setup) method for finding and resolving anomalies. The Honeycomb licensing model should result in lower costs. Installation and management of OpenTelemetry agents and collectors may complicate the initial setup, but the use of OpAMP enables easier day-to-day management of collectors and agents. A sandbox allows users to understand the basics of Honeycomb easily and provides developers with a place to test code before going to production.

Challenges

Honeycomb focuses on observability for DevOps and engineering teams, while other players take a broader view of IT operations. As Honeycomb grows, these limitations will become less significant. Predictive analytics are limited to SLOs using events.

Purchase Considerations

The tiered subscription license model comes with a free option that includes 20 million events per month. The Pro and Enterprise tiers come with increased limits. Volume limits apply to each tier, and licensing is by event. A log file may include an event per line, which can eat licensed events quickly, but Honeycomb has a burst-protection feature to notify users of overages. Data retention is 60 days.

Enterprise-tier customers can negotiate longer data retention.

Honeycomb markets to pro-coders and engineers in any size organization. Much of its technology is based on open source software, but because it markets to technical users, open source skills are less of a constraint than with other open source observability vendors. Honeycomb provides a sandbox demo to allow potential customers to see and use the solution.

Honeycomb has vertical support for online gaming development. Any enterprise with high-cardinality data can use Honeycomb to sift through and “bubble up” the data that matters. Additionally, traces can be tailored to the organization’s needs rather than attempting to consume and analyze all the data from a trace. Developers are the target, and the closer an organization is to “testing in production,” the more likely Honeycomb may be on the shortlist for cloud observability solutions.

Radar Chart Overview

Honeycomb is in the Innovation/Feature Play quadrant due to novel features like BubbleUp, the use of LLM query analytics, and the heavy use of open source. The company focuses on the needs of developers rather than IT in general.

IBM: Instana

Solution Overview

IBM Instana is a SaaS observability solution that can host almost anywhere, including natively on IBM Cloud, and on AWS, Oracle Cloud, and Google Cloud Platform (GCP). It can also be self-managed on-premises. Open standards supported by Instana include Prometheus, StatsD, OpenTracing, OpenCensus, Jaeger, W3C Trace Context, and DropWizard. And, as it is part of IBM’s immense portfolio, any feature not available directly from Instana can be found in another IBM product.

Instana’s dashboards are exceptional—consistent, customizable, and shareable—and a no-code monitoring tool, Application Perspectives (AP), allows the creation of dashboards tailored to a particular user or group. In addition, Instana’s AutoProfile lets users analyze code-level performance, discover bottlenecks in production code, and visualize performance with a unique flame graph. User performance monitoring ticks all the boxes with real user monitoring, synthetics, and a Synthetic Point of Presence (PoP) that can be placed anywhere.

Also superior is Instana’s multicloud functionality—in any cloud, anywhere. Its pushing data and tagging capabilities are average and use OpenTelemetry or API calls. The IBM platform is comprehensive, so it’s surprising that LLMs and predictive analytics were not included. However, IBM Watson Cloud Pak offers LLM support, and predictive analytics is available from IBM Cloud Pak for AIOps.

Instana has average scores for edge observability and identification of ghost changes. However, it supports both edge computing and PoP synthetics, allowing full edge observability. Tools are available for edge computing and observability, but each organization will have to determine the configuration details to handle the compute portion—it’s a build-your-own scenario. Instana can be set up to look

for configuration changes and send alerts. Multiple steps and careful configuration are required to detect changes in applications and infrastructure, though with good potential.

As expected, IBM did very well on our business criteria, with only cost receiving a less than superior rating. The IBM ecosystem is exceptional, covering all requirements and adding TechExchange for the Instana community. Deployment for SaaS is straightforward, with many data ingestion possibilities for enterprises that are worldwide or employ diverse application environments. The on-site version of Instana is relatively uncomplicated and includes excellent documentation and support. Ease of use is first rate with consistent and intuitive dashboards. Agility is enhanced with Instana's AI-driven data contextualization.

Strengths

Instana has a number of strong features, including dashboard creation and management, user interaction performance, multicloud capabilities, and the ability to consume and send tags. Deployment is uncomplicated for both SaaS and on-site, though the latter can be more time-consuming. Instana itself is easy to use and integrates with almost everything.

Challenges

LLM and predictive analysis are available only via IBM Watson Cloud Pak and IBM Cloud Pak for AIOps, which can be integrated with Instana at an additional cost.

Purchase Considerations

Security features include the standard SSO and RBAC capabilities, plus connection to almost any certificate or password store available. Costs are per host per month, billed annually, which is considered average. A free 14-day trial is also available.

Instana can be a compelling alternative to the traditional leaders in cloud observability. As an IBM offering, it brings the power of one of the largest technology companies in the world. Any enterprise invested in IBM solutions should shortlist this offering, try the free version in a test lab, and compare the results to the leaders. The scales may not balance completely, but considering IBM has never been a bad idea.

IBM targets all size organizations, but larger enterprises, including several vertical markets such as healthcare, banking, and manufacturing, are the focus of IBM marketing.

Radar Chart Overview

IBM's Instana is a well-known product from one of the world's largest platform players, and the company is thus positioned in the Maturity/Platform Play quadrant. IBM is a Forward Mover with new releases on a roughly yearly basis.

LogicMonitor: LM Envision

Solution Overview

LogicMonitor's LM Envision is an automated monitoring and observability platform targeted at enterprise IT and managed service providers (MSPs). The unified

platform provides end-to-end tracing with code-level visibility across the entire stack; seamless data collaboration at scale; visibility into networks, clouds, containers, applications, servers, and log data; and AIOps for metrics, logs, and applications. LM Envision provides capable synthetics and traces with topology mapping for AWS and Azure deployments.

In addition to its predictive and AIOps capabilities, the LogicMonitor roadmap indicates the expected general availability of its LLM solution, Admin Co-Pilot, at the end of the first quarter of 2024. The purpose-built generative AI will be pretrained on LogicMonitor APIs to help them perform administrative tasks on the platform. Many vendors in the cloud observability space are currently previewing their LLM solutions, so LogicMonitor is considered average in this key feature.

LogicMonitor deploys using an agentless solution that does not require installing agents or other code on every monitored resource. But you do install LogicMonitor Collector, a 100 MB Java application, on hosts within your infrastructure, and it then monitors resources using standard protocols. REST APIs and SDKs also allow customers to push metrics, logs, and traces to the platform. LM Envision is able to use any metadata sent with metrics or telemetry to enrich the data and provide additional context. LM Envision can provide superior predictive analytics and forecasting for up to one year, with decreasing accuracy with a smaller historical data set or for longer prediction times into the future.

Edge observability is not specifically supported. With the use of private location synthetics, the beginnings of a solution are possible, but the lack of edge computing leads to a poor grade. Identification of ghost changes is, however, a strong area for LogicMonitor with the ability to use LM Config (part of LM Envision) to baseline and highlight configuration changes across networks, systems, storage, and other assets; alerts are then provided when unexpected changes occur. Additionally, for Kubernetes, Logic Monitor's LM Container monitors changes in the configurations of Kubernetes objects. LM Container can set alerts based on configuration value changes and create a backup copy of the Kubernetes object configuration.

Ease of use is average, with a consistent UI throughout the product. LogicMonitor offers a significant library of out-of-the-box dashboards that can be shared across users, with prebuilt dashboards following best practices for various industries, including financial services, health and life sciences, manufacturing, retail, education, state and local governments, software companies, and service providers. The no-code environment includes a widget to simplify the modification of new dashboards and creation of new views.

LogicMonitor has over 2,500 prebuilt third-party integrations for cloud, network, storage, servers, and databases, allowing businesses to integrate quickly with the devices, technologies, and services they rely on. LogicMonitor's score on the ecosystem metric is average, but it does offer training, certifications, a partner program, community forums, and online documentation. LM Envision supports SSO, RBAC, and two-factor authorization. All sensitive data uses encryption both in transit and at rest.

Strengths

LM Envision has superior strength in multicloud functionality and predictive analysis, which can forecast up to a year in the future. The solution supports the main public clouds as well as private clouds and walled gardens. The use of low-code for dashboards and administration contributes to the solution's ease of use. Finally, with changes in software and infrastructure being the primary cause of service interruptions, the use of LM Config to see changes made outside the change-management process is a better than average feature.

Challenges

LM Envision lacks support for edge observability, but the use of private location synthetics is a starting point. LLM support is on the roadmap but not yet available.

Purchase Considerations

Pricing is determined by the number of devices or resources monitored per month and organized by standard resource licenses, MSP licenses, cloud monitoring, and MSP licenses for cloud monitoring. Components of the LM Envision offering, LM APM is sold by the number of invocations or checks and LM Logs is sold as an add-on by volume of logs collected and duration of storage. Dexda is an add-on license to the subscription and is measured by number of insights per month. SaaS application monitoring is also sold separately. Professional services, support, and customer training are offered as additional packaged bundles.

LogicMonitor markets to any size organization. However, the majority of its sales are to mid-market companies. Smaller companies should look closely to determine whether LogicMonitor fits their needs before adding them to their shortlist of vendors.

LogicMonitor has broad support for many industries. Vertical support includes financial services, health and life sciences, manufacturing, retail, education, state and local, software companies, and MSPs. SMBs, enterprises, and MSPs are common users of LogicMonitor.

Radar Chart Overview

LogicMonitor is a Fast Mover because product feature releases occur every three weeks. Product updates are aggregated and announced to the market on a quarterly basis. That, and LM Envision's platform architecture, puts the company in the Innovation/Platform Play quadrant.

Microsoft: Azure Monitor

Solution Overview

Microsoft Azure Monitor collects and aggregates data from all layers and components, across multiple Azure and non-Azure subscriptions and tenants. It stores data in a common platform for consumption by a shared set of tools that can correlate, analyze, visualize, and respond to what the data shows.

Microsoft provides all the necessary tools for creating, customizing, cloning, and sharing dashboards and reports. Traces and user monitoring are supported, as are private locations for private clouds and walled gardens. Availability tests are possible using the TrackAvailability functionality, which allows the creation of a

custom application to run availability tests, which can simulate synthetic transactions. These are not synthetic transactions, however, as multistep web tests (synthetics) have been deprecated.

Azure Monitor is only cloud-native on the Azure platform. While organizations that are Microsoft-centric may have the majority of their applications running on Azure, they may also have applications running in other public or private clouds. The lack of native support for those other clouds may complicate using Azure Monitor. It is possible to integrate other Microsoft and non-Microsoft tools, and Azure allows data from other clouds using OpenTelemetry. Azure Monitor allows data to be tagged with OpenTelemetry and can use API calls to push or pull metadata tags. This is standard in the market. However, cloud resource data is available only for Azure, resulting in a poor rating overall.

Predictive autoscaling uses ML to help manage and scale Azure Virtual Machine Scale Sets with cyclical workload patterns. This forecasts the overall CPU load of a virtual machine (VM) based on historical CPU usage patterns. This process ensures that scale-out occurs in time to meet demand. Predictive autoscaling needs a minimum of seven days of history to provide predictions. The most accurate results come from 15 days of historical data for up to 24 hours of forecasting. While Microsoft supports and funds OpenAI, Azure Monitor currently makes no mention of it.

Azure Monitor does not offer much for edge observability beyond the edge of the Azure cloud, resulting in a poor score. Regarding ghost changes, the Microsoft Change Analysis tool provides data for various management and troubleshooting scenarios to help diagnose what changes to your application caused issues. Changes are events that occur in your Azure application, from infrastructure through application deployment, which are traced at a subscription level. This increases observability by building on the power of Azure Resource Graph to provide more detailed insights, contributing to an average rating.

Microsoft's ability to satisfy operations needs results in superior scores on all business criteria except cost. Ease of deployment is fine since Azure Monitor is a SaaS solution. Collectors and agents are handled with relative ease within Azure, but more work is necessary for other public clouds and on-premises applications. Ease of use is helped by a consistent UI across a large, complicated system. Most changes are low-code, but some administrative and set-up tasks require pro-code skills. Much of Azure Monitor is fixed, leaving users unable to customize to their needs. On the other hand, there are many integrations, many templates, and copious documentation.

Strengths

Microsoft's strengths in monitoring the Azure Cloud are sufficiently advanced that the key features for this Radar only scratch the surface. Regardless of the overall average scoring for key features, they are more than sufficient for any Microsoft shop. Unusually, compared to other vendors, Microsoft has the ability to find ghost changes. The depth may not be as great as a standalone configuration change tool but is certainly a standout in the cloud observability marketplace. Deployment, ease of use, agility, and security are excellent due to Microsoft's keen

understanding of their clientele. The Microsoft support ecosystem is exceptional, as should be expected.

Challenges

Unsurprisingly, Azure Monitor is less than perfect in observing non-Microsoft cloud environments, but it can monitor applications using OpenTelemetry. The focus on Azure Cloud also limits edge observability to the Microsoft world.

Purchase Considerations

Correlating different data types may be complex due to differing time increments and incompatible data resolution depending on the data source and ingestion rates. Azure Monitor Application Insights supports codeless/agentless auto-instrumentation for applications developed in languages such as Java or the Microsoft .NET platform. The Microsoft ecosystem is broad and comprehensive, with support across training, certification, forums, professional services, and online documentation.

Cost is based on ingested data and retention time. A cost calculator is available to help assess costs and keep them contained. The Microsoft license model is based on consumption pricing that includes logs metrics, alerts notifications, web tests, and system center operations manager (SCOM) managed instances.

Any organization using only the Azure cloud should pay strong attention to Microsoft. After all, it is their turf where they have a home-field advantage. On its own, this is enough for any enterprise to look at Microsoft as their observability vendor.

Microsoft has always catered to any size organization, and Azure Monitor is no different. SMBs, large enterprises, and service providers are all marketing targets and valid customers.

Radar Chart Overview

Microsoft is positioned in the Maturity half because Microsoft is a well-established company with decades of experience and Azure Monitor has a depth of capabilities only a long history of development can create. It is on the Feature Play side of the Radar because the focus on Azure Cloud makes Azure Monitor applicable to fewer use cases.

New Relic

Solution Overview

The New Relic SaaS observability platform has more than 30 capabilities and 750 out-of-the-box integrations. It can ingest metrics, logs, and traces from any source, including public, hybrid, and private clouds.

New Relic earns an exceptional score on the user interaction performance and dashboard and reporting metrics. Dashboards are customizable, with numerous visualizations and customizations available. Users create dashboards using low-code/declarative templates. New Relic supports RUM, synthetic transactions, transaction tracing, transaction replies, and a navigable topology map.

The New Relic platform provides a unified view of all cloud resources from public

or private clouds. Clouds can be viewed individually or in groups, giving the solution a superior score in this key feature.

New Relic AI (NRAI) is in public preview (open beta) and is available to all New Relic customers free of charge. (The only exception is the small group of FEDRAMP and HIPAA-enabled accounts that are ineligible to use NRAI.) It uses Azure OpenAI's GPT-4 Turbo with full-stack insights, automated health checks, and system optimization without the learning curve. Its functionalities include onboarding assistance, natural language querying, root cause analysis, code debugging down to the line of code in the IDE, and reporting. For privacy and safety, the LLM does not have direct access to the New Relic databases—the LLM is used to compose a New Relic query language (NRQL) query, which NRAI then runs against the New Relic Database (NRDB).

New Relic has superior pushing and tagging, which allows users to add metadata to their data in the form of tags to categorize and filter information. Details can be pushed using out-of-the-box integrations or using an API. New Relic is a real-time system and has minimal ability to predict future states of metrics and events, which results in a low score for predictive analytics. New Relic detects anomalies, creates possible root cause determination, and finds alert correlation from real-time data. The company's roadmap includes improvements in forecasting and predictive performance analysis.

New Relic also garnered a superior rating with its support for edge observability. Collectors can be placed at the edge for synthetic transactions. Edge computing power comes from Kubernetes using Pixie, an open source observability tool for Kubernetes applications. New Relic Edge provides tracing on Kubernetes workloads at the edge using eBPF to gather data. Auto-telemetry with Pixie data and security leverages Community Cloud for Pixie, a separate platform from New Relic. New Relic does not support the discovery of ghost changes outside of planned changes and those that follow a process.

New Relic receives a superior rating on all of the business criteria for cloud observability. The platform is provided as a managed SaaS service. Guided installs use the New Relic command-line interface (CLI), the infrastructure agent for the host environment, and installation recipes to instrument applications and infrastructure. Jenkins, Chef, and Puppet are integrated automatically. The New Relic platform can be considered no-code or low-code, meaning it is fairly easy to use. There are rare occasions when a more sophisticated pro-code approach is needed.

Customization of the main landing page allows pinning of features used most often, enhancing ease of use. For organizations that have more than one account, the account switcher displays the current account and allows switching accounts at any time. Global search allows searching for entities such as monitored services, monitored hosts, and custom dashboards. New Relic charts and pages are shareable.

The ecosystem includes New Relic University, which offers onboarding and training resources and is free for all customers and partners. Badges and

credentials can be obtained as well. Guidance from the Observability Center of Excellence (OCoE) helps customers establish an observability team in their environments that focuses on best practices. Observability maturity practices are tutorials that train these teams to tailor plans to the customer's business goals. The Customer Onboarding Framework trains New Relic partner teams in implementation and training. Online documentation, community forums, hands-on tutorials, virtual and instructor-led training webinars, and workshops, plus certifications are available. The New Relic partner program consists of more than 1,000 global partners, and New Relic supports a public community forum: The Explorers Hub.

New Relic supports SSO using ADFS, Auth0, Azure AD, Google, Okta, OneLogin, Ping Identity, and Salesforce. New Relic can drop sensitive log data at ingest. The use of New Relic Vulnerability Management enables additional capabilities by identifying vulnerabilities automatically and alerting and managing threats.

Strengths

New Relic continues to have exceptional strengths with its dashboard and user interaction performance, which have improved both in features and in the ability to customize the environment to suit the user. All public clouds are handled well, with native AWS, GCP, and Azure code. On-site support is good, using container images to collect and process data before forwarding to the SaaS solution. New Relic is also strong in business criteria. Deployment is straightforward and well-supported. Ease of use has improved, with further improvements on the 2024 roadmap. New Relic is an agile platform that can be customized to integrate with enterprises using a mostly low-code environment. Security is becoming increasingly important to enterprises and is handled with integrations to common password vaults, and New Relic Vulnerability Management helps identify and alert on known exploits

Challenges

New Relic has minimal support for discovering ghost changes to infrastructure using pro-code—improving this capability would allow New Relic to move significantly beyond most observability vendors.

Purchase Considerations

Most tools in the New Relic portfolio are available in the free version, and the entire platform of features is accessible in higher tiers. The New Relic pricing model is usage-based for users and data ingest. There are a number of usage tiers, including free, Standard, Pro, and Enterprise. Pricing has become more nuanced with new data consumption levels, including longer data retention, a greater query limit, and a greater choice in public clouds. New Relic Vulnerability Management is included with the Pro and Enterprise tiers. Support SLAs increase with the tiers, with Standard and Pro tiers at two hours and the Enterprise tier at one hour for the initial response.

The New Relic licensing tiers include a perpetually free tier with no credit card required. The standard tier is for small teams with eligibility for Data Plus. The Pro Tier is for teams with more than a few engineers and complex workloads, and no maximum for the number of provisioned users with eligibility for Data Plus (which

provides advanced performance, scaling, and governance capabilities). Finally, the Enterprise tier is the Pro tier plus FedRAMP Moderate, HIPAA eligibility, priority ticket routing, and eligibility for Data Plus.

Customers are billed based on the volume of data ingested, measured in gigabytes. There are two ingest bundles: the original data bundle and the Data Plus bundle (Pro and Enterprise tiers only), which has longer data retention and higher query limits and query durations.

New Relic is a major vendor in the cloud observability marketplace. Ease of use and rapid deployment have always been strong and remain a reason to shortlist New Relic. Its LLM support is developing rapidly, with more features on the 2024 roadmap. Predictive analytics is a weakness for New Relic. Perhaps the LLM tools will mute this limitation and enable the company to be considered by those in need of forecasting and predictive analysis. Licensing has subtle changes that do not keep New Relic from being a contender.

New Relic can target any size of business. Their free offering allows smaller companies or projects to use an observability product with good functionality while limiting users, data consumption, and support. The higher tiers, Enterprise in particular, provide access to the entire scope of New Relic.

Radar Chart Overview

New Relic is positioned in the Innovation/Platform Play quadrant. Its past and projected release cadence (over 40 releases in 2023 and 50 product updates broken into three major launches and 10 minor launches per quarter for 2024) classify it as an Outperformer.

OpenText: Operations Bridge

Solution Overview

Operations Bridge (OpsBridge) from OpenText monitors the IT environment and consolidates and normalizes data from third-party tools. OpsBridge applies automated discovery, monitoring, analytics, and remediation to data across traditional, private, public, multicloud, and container-based infrastructure. It automates AIOps with ML and analytics, which reduces events and improves root cause identification and remediation.

OpsBridge has superior out-of-the-box reports and dashboards to communicate service health to stakeholders and operations users. Dashboards come in two flavors. First, Stakeholder dashboards are built with standard Office tools (even Visio, a unique feature among vendors). These can contain infographic dashboards that can include live video, social media streams, and more. Second, Flex dashboards are built within the tool by dragging and dropping widgets. Both kinds of dashboards are customizable, shareable, and built using low-code environments.

RUM is also superior and captures end-user performance and availability. OpsBridge offers synthetic transactions and transaction tracing. The solution also has a navigable topology map of services and applications. The solution includes Hybrid Cloud Management X (HCMX), which delivers cloud cost optimization

(FinOps) via multicloud spend reports for AWS, Azure, and GCP, resulting in capable multicloud functionality. It also delivers AI-powered recommendations for savings (commitment-based discounts) and budget management with alerts and tracking.

Predictive analysis is superior, with forecasts up to 14 days out using multiple algorithms. Best results are achieved with at least three months of historical data. OpsBridge LLM support will be released in 2024 based on an OpenText initiative called Aviator. This is considered average at the current stage. Pushing and tagging data are supported by consuming metadata and pushing tags using source APIs.

OpsBridge does well in edge observability with a capable solution featuring synthetics, remote probes, client-side instrumentation, and edge computing using their recently introduced App Observability product. Identification of ghost changes is similar to most observability vendors: poor.

OpenText OpsBridge has superior deployment options, with a SaaS-based product and an on-premises offering. Monitoring can be either agent-based or agentless, which uses SiteScope. OpenTelemetry-based capabilities are a primary focus of ongoing development. Integration using APIs allows customers to use products like Terraform to deploy via automation.

Day-to-day ease of use is superior due to out-of-the-box methods to ingest data, including an integration hub and a wizard. Automated discovery and automated event correlation are standard features. For the SaaS offering, all updates—except agents—are performed by the OpenText SaaS operations team. On-premises updates are packaged by OpenText for use by administrators.

API-based monitoring-as-code enables developers to build monitoring directly into their applications as they are deployed. Dashboard and report creation uses a drag-and-drop no-code environment; users do not need to know SQL. The majority of OpsBridge functions have callable CLIs for use by pro-code developers. OpenTelemetry libraries are available for automatic instrumentation or manual instrumentation of applications.

The agility of OpsBridge is excellent and allows enterprises to be flexible in the DevOps process and the implementation of OpsBridge, which has a superior array of capabilities for various resources and personas. Training and certifications are available. The partner program offers co-marketing and education, a public community forum, and an independent user community.

Strengths

OpsBridge offers dashboards with both stakeholders and operational staff in mind, using a low-code environment for both. User interaction performance covers everything from RUM to synthetics. Predictive analysis can extend to 14 days and provides better quality with more historical data. Edge observability is better than expected, with tooling to handle mobile devices. Ease of deployment is good for both the SaaS and on-premises offerings. Ease of use is strong, with a consistent interface and no-code and low-code customization. The agility of OpsBridge is also strong due to the flexible DevOps requirements and integration possibilities.

Finally, the ecosystem contains everything any enterprise may need for support.

Challenges

LLM support is not as advanced as most vendors, but the additional time may produce a better product. The identification of ghost changes is limited, which is not unusual in the current observability marketplace.

Purchase Considerations

OpsBridge is a single product with multiple modules that can be selected based on need. It is built on the OPTIC platform, a data lake for rapid data ingestion of data. It can be deployed on-premises or consumed as a SaaS service from OpenText. Licensing is in units consumed according to the number of agents, agentless, synthetic, and real user monitoring usage. Customers can switch the use of the units at any time. Subscription and perpetual licenses are available.

OpsBridge is not a product for SMBs, and OpenText is clear it markets to larger enterprises and service providers only. There are notable features in OpsBridge that most vendors don't have and its ease of use is compelling. The distinction between stakeholders and operations is an important consideration for larger businesses. Edge observability is also more of a concern for larger organizations, and OpenText has a viable solution. OpenText supports too many vertical industries to list here (more than 20). Potential users should check whether their industry has specific tooling or support from OpenText.

Radar Chart Overview

OpenText is positioned in the Maturity/Platform Play quadrant as it's a large platform-orientated company that's applicable to many use cases. It's classified as an Outperformer due to its above-average rate of change. It has a compelling feature set that should help it move more quickly to challenge the Leaders.

ServiceNow: ServiceNow Cloud Observability

Solution Overview

Cloud Observability is a relatively new product for ServiceNow, made possible by the acquisition of Lightstep. The tool collects and analyzes telemetry data across infrastructure, applications, runtimes, clouds, and other third-party services. ServiceNow Cloud Observability is a SaaS-only product with agents for on-premises data collection. ServiceNow uses microsatellites (its own proprietary collectors) and makes use of OpenTelemetry for MELT.

ServiceNow Cloud Observability offers three types of microsatellites, each used at different times during the development lifecycle. A local developer mode satellite is installed on a local machine and used like a sandbox when developing services. Public microsatellites are a shared pool of microsatellites managed by the Cloud Observability solution. On-premises microsatellites are installed and run in the enterprise environment. In addition to these methods to ingest data, organizations that have adopted OpenTelemetry can point their collectors at ServiceNow for ingestion and analysis.

For production environments, microsatellites provide data from the entire enterprise. They can be downloaded, installed, and tuned to fit a specific need.

Microsatellites are straightforward to deploy using a Docker image, AWS AMI, or Debian package. Cloud Observability integrates with Amazon and uses CloudWatch Metric Streams to send metric data into its system, using OpenTelemetry Collectors to ingest metrics from Azure Monitor. Clusters running inside Azure's managed Kubernetes service can be configured to emit detailed metrics in OpenTelemetry format. An integration with GCP sends cloud monitoring (including custom metrics) to Cloud Observability. Cloud Observability supports Python, Go, Java, Node, C++, Ruby, .NET, and other common programming languages and platforms.

Digging into the key features, ServiceNow Cloud Observability shows a few superior and some unexpected problematic areas. Dashboards can be created, edited, shared, cloned, marked as favorites, and have other capabilities, giving them a superior rating. They can be created via both drag-and-drop and templates. There are service health dashboards for individual services and dashboards that allow the user to select from all available services. Prebuilt dashboards can receive data from AWS CloudWatch Metric Streams, Azure, or a metric integration using the OpenTelemetry Collector.

User interaction performance is monitored with OpenTelemetry traces. Synthetic transactions are not a specific part of the solution; however, agents can do ping tests to verify connectivity. As a result, this just meets the average score. Multicloud support is superior, with the ability to consume data from anywhere as long as a collector can be installed using Docker. ServiceNow has LLM capabilities in the Now Intelligence product that Cloud Observability can't use, which results in a poor score. Consuming tags (attributes in OpenTelemetry) is average, and with APIs, tags can be pushed where needed. Predictive analytics is not a part of Cloud Observability, but it can be achieved using the Service Graph Connector and a subscription IT operations management (ITOM) Visibility application or the ITOM Discovery application.

Self-managed deployment is well-structured with clear instructions a skilled system administrator can handle. SaaS deployment is also not difficult. On-premises microsatellites for production environments provide complete control over the installation. They are straightforward to deploy via numerous methods noted above. Additional steps exist to integrate collaboration tools (Slack) or other products. Not all deployment details have been discussed, but overall, the deployment process meets the requirements for a superior rating. The agility of the solution is also superior.

ServiceNow Cloud Observability is not fully integrated into the ServiceNow Platform, which results in a bit of a learning curve. However, Cloud Observability is better and more usable out of the box than other ServiceNow offerings. The UI is consistent and uncomplicated. Many functions can be handled by low-code or no-code tools. Pro-code skills are necessary for some administrative, integration, and configuration tasks, but the impact is low. Ease of use is good in ServiceNow Cloud Observability.

The ability to tweak a product to fit the needs of the enterprise without extensive pro-code modifications is significant, and it's one Cloud Observability handles

exceedingly well. Some terminology may be odd—microsatellites are proprietary collectors from ServiceNow. Their function is the same as other collectors but tuned to ServiceNow needs. OpenTelemetry collectors are supported, and ServiceNow is a contributor to the open standard.

ServiceNow is known for its exceptional ecosystem of support. While Cloud Observability is a newer product for ServiceNow, it is a full part of the extensive ServiceNow ecosystem.

ServiceNow integrates with existing security tools such as Azure AD, Okta, or OneLogin to manage users and roles in Cloud Observability. It allows user access control with RBAC and lets identity providers (IdPs) authenticate users through SSO. Cloud Observability can manage users and roles at scale with JIT provisioning, the Cloud Observability API, Okta, the System for Cross-domain Identity Management (SCIM) protocol, or Terraform.

The microsatellites and OpenTelemetry Collectors are plain binaries that only process the data explicitly sent to them by the tracer instrumentation. The microsatellite or collector does not automatically inspect, acquire, or otherwise gather data from the host environment. As such, you have complete control over what data is accessible. Data is encrypted on the move and at rest. Cloud Observability complies with SOC2 and GDPR.

Strengths

Cloud Observability has dashboards that are uncomplicated and easy to use. Multicloud functionality is also good, with native support for most public clouds and either a hybrid model or a self-managed offering for on-site clouds. The solution is easy to deploy from an on-premises perspective and for the SaaS offering. Of note is how agile Cloud Observability can be with its flexible processes and manageable integrations. And more broadly, ServiceNow has many strengths as a company, including an excellent support infrastructure.

Challenges

Two of the challenges for Cloud Observability are surprising—it's lack of an LLM and of predictive analytics. ServiceNow does offer an LLM called a Now Intelligence, but it is not connected to Cloud Observability. And predictive analytics, which is available in other ServiceNow products, is not present here. These omissions are off-putting: they do not suggest the product is defective, but it is surprising that these are not yet integrated into the full ServiceNow platform. Support for edge observability is limited to simple pings. The ability to see ghost changes is missing.

Purchase Considerations

Licensing is available for two editions. The Teams Edition comes with a maximum of under 2,000 subscription units allowed per month with a monthly billing period. The Enterprise Edition has unlimited subscription units allowed and is billed annually. A subscription unit is a shared unit of measure. Each managed cloud observability resource type is counted toward a subscription unit based on predefined ratios.

Other data types, such as Active Time Series, Trace and Log Data Ingest, Log Data

Hot Retention, and Log Data Cold Retention, use similar units. The unit of measure for Metrics is Active Time Series, timestamped measurements that share a metric name and a unique set of tag keys and values for 13 months. Each subscription unit costs \$1. Volume discounts are available for Enterprise Edition customers.

ServiceNow is an enormous platform. Enterprises heavily relying on it in other areas (ITSM, CMDB, ITOM) should consider Cloud Observability as a straightforward addition. While it is a recent acquisition, the software will become more connected to the overall platform over time. Non-ServiceNow users may wish to consider Cloud Observability by itself due the strong features it has now and the expectation they will only get better.

Those already invested in OpenTelemetry will find that moving to another vendor with full support for the standard will be painless, as it should be. Cloud Observability has good support for DevOps teams.

Radar Chart Overview

ServiceNow has one of the most complete IT support platforms in the marketplace. Additionally, even though Cloud Observability is available through the recent acquisition of Lightstep, it is a mature product from a mature company. These factors place Cloud Observability solidly within the Maturity/Platform Play quadrant. Also, the update cycle for Cloud Observability shows 13 updates before the middle of February 2024, marking ServiceNow as an Outperformer in this space.

SolarWinds: SolarWinds Observability, Hybrid Cloud Observability

Solution Overview

SolarWinds is an IT service management, application performance, and database management solutions provider. It offers two versions of its cloud observability platform: SolarWinds Observability, a SaaS solution with native support for AWS and Azure, and SolarWinds Hybrid Cloud Observability, which is integrated with and provides visibility to SolarWinds Observability via SolarWinds Platform Connect.

Most key features in SolarWinds Observability receive average ratings, with multicloud functionality and dashboards registering superior scores. The product includes prebuilt system dashboards and custom dashboard templates that can be edited in a low-code environment. Hybrid Cloud Observability enables its own users and non-SolarWinds users to share dashboard views. Synthetic transactions (including private locations) and RUM are supported along with tracing from OpenTelemetry.

Multicloud support for Azure, GCP, or AWS clouds uses agentless integration, while other clouds require agents or collectors for data ingestion. SolarWinds can receive metadata from any data source and can push information using its APIs. Historical data, multidimensional baselining, and forecasting are used to provide recommendations for fixing current and predicted issues through automated actions, covering the predictive analysis criterion.

SolarWinds assists in enabling edge observability. The Hybrid Cloud Observability product can monitor and report on IoT and edge devices using synthetic transactions and collectors with computing power to analyze and condense data before forwarding it to the main SolarWinds installation. There is support for detecting ghost changes. SolarWinds has automatic and manual baseline comparisons of network configurations and databases. These can identify unauthorized changes made to the system, including alerting when changes occur, and changes can be rolled back to a known baseline. The SolarWinds roadmap includes expanding management and alerting of policy and infrastructure changes across the observability stack in 2024.

Ease of use is superior. The UI is undemanding and consistent throughout the products, and users can make changes using low-code tools. SolarWinds solicits customer feedback on ease of use and features through in-product feedback. The SolarWinds solutions are customizable via no-code and low-code features and receive a superior score for agility. Users can leverage the API and SDK for advanced functionality. OpenTelemetry enables further extensibility, as SolarWinds supports and contributes to that open source framework.

Out-of-the-box prebuilt integrations cover applications, infrastructure, logs, and integrations with third-party products. Developers can extend functionality using Telegraf, public APIs, and custom metrics. SolarWinds has a superior support ecosystem with online documentation, training, certifications, public forums, and a SolarWinds-sponsored online community, THWACK, with almost 200,000 members.

Security includes a dashboard and risk scorecard in addition to the more common SSO, RBAC, and multifactor authentication (MFA) features, resulting in a superior rating. SaaS and self-hosted observability solutions are sold via subscription licenses. Cost is considered average.

Strengths

SolarWinds Observability can be natively deployed on AWS or Azure. The self-managed SolarWinds Hybrid Observability can also be installed on-premises or on AWS and Azure, providing customers with flexible deployment and management options. The solution is easy to use wherever it is deployed, with no-code and low-code interfaces, and it also integrates well using the API. The ecosystem hits all the marks and includes the strong THWACK online user community. Security is particularly pleasing due to the vulnerability dashboard and risk scorecard. All other key features and business criteria are capable with no glaring weaknesses.

Challenges

There is no native support for GCP, though monitoring and metrics can be consumed from that environment with OpenTelemetry agents and collectors.

Purchase Considerations

Both SolarWinds Observability and Hybrid Cloud Observability are fairly easily deployed. The SaaS deployment is uncomplicated, while deploying Hybrid Cloud Observability on-premises requires a bit more time and effort. SolarWinds has automated the deployment of agents. Updates and upgrades are seamless with

the SaaS installation. Self-hosted users receive three to four releases of combined updates per year.

SolarWinds Hybrid Cloud Observability (self-managed) is licensed by the number of nodes. SolarWinds Observability (SaaS) offers license subscriptions sold annually or monthly based on a combination of features—APM, synthetics, RUM, networking, logs, infrastructure, and database applications, each measured in its relevant consumption units.

In vertical markets, SolarWinds has a long history with federal, civilian, and defense organizations, state and local governments, education, financial services, and healthcare. Users in these areas should consult with others in the vertical.

Radar Chart Overview

SolarWinds is a mature company with a long history of providing monitoring and is positioned in the Maturity/Platform Play quadrant. It has a capable product and solid scores across the decision criteria we evaluated and is classified as a Leader. The speed of feature delivery classifies SolarWinds as a Forward Mover.

Splunk: Splunk Observability

Solution Overview

Splunk Observability, comprising Splunk Platform and Splunk Observability Cloud, can be consumed through a SaaS-only model in Splunk Cloud (hosted in AWS or GCP) and via an on-premises deployment of Splunk Enterprise. Splunk Observability Cloud is available through a SaaS-only model and includes application performance monitoring, infrastructure monitoring, network monitoring, real user monitoring, synthetic monitoring, and point-and-click log analysis. The Splunk Platform provides log ingestion and analytics for IT operations (ITOps) and engineering teams (including security analysts). The two versions, Splunk Observability Cloud and Splunk Platform, have similar but not identical feature sets. For instance, the Splunk Enterprise Security and Splunk IT Service Intelligence (ITSI) add-ons are only available on the Splunk Platform.

Splunk Observability provides preconfigured dashboard templates for ITOps engineers, site reliability engineers (SREs), and developers. The Splunk distribution of the OpenTelemetry collector automatically enriches metrics, traces, and logs with infrastructure metadata. Splunk Platform users can enrich the data with lookups and create more meaningful visualizations.

Splunk's RUM in Splunk Observability Cloud analyzes every user session from web pages and native mobile (iOS and Android) applications and stitches them together with their dependencies on backend services and third-party components. Splunk Synthetic Monitoring allows customers to validate complex multistep user flows and business transactions. Private locations allow synthetics to be used within customer firewalls.

Cloud resources can be displayed individually, in combined dashboards, and with free Splunkbase apps for more granular inspection. Splunk Observability dashboards and reports are highly customizable and can be arranged and configured to visualize specific layouts and specific data.

Data can be consumed and pushed to other ITOps platforms, such as ServiceNow and PagerDuty. Custom metrics provide complete flexibility to add and process any kind of data, including financial operations.

Customers can use alert rules in Splunk Observability to predict outages by identifying outliers in a population, historical anomalies, and sudden anomalies, all driven by predictive analytics. Metrics and alerts integrate into Splunk ITSI, which supports adaptive thresholding and predictive analytics of business service health up to 30 minutes in advance of potential service disruptions using ML algorithms and historical service health scores. Service health predictions require a minimum of 14 days of data (30 days are recommended).

Splunk provides exceptional capability in edge observability. Splunk Edge Processor and Ingest Actions can filter, mask, and transform data close to its source prior to ingest, thus minimizing data transport and allowing problem identification before leaving the customer's network. before routing the processed data to external environments. The final link in edge observability is Splunk Synthetic Monitoring (with or without private locations), which can proactively monitor site availability before it affects users, report on the availability or impact of third-party services, check how new code deployments improve or degrade performance, and scan for moved or broken links.

With regard to ghost changes, Splunk can identify infrastructure changes and changes in service topology. Software and other configuration changes can't be seen.

The deployment of the Splunk Observability Cloud is easy, with only customer signup required to deploy collectors and agents. Splunk Enterprise does require some work, as infrastructure must be procured. There is a single UI but two admin consoles, one for Splunk Enterprise and a second for Splunk Observability. Splunk Observability delivers a superior integrated no-code user environment to view infrastructure and application metrics and troubleshoot issues. More advanced users have full control with Splunk's Search Processing Language (SPL) and SignalFlow queries, but any user can leverage hundreds of out-of-the-box integrations, dashboards, and alert rules.

A Splunk navigator is a collection of resources that enables the monitoring of metrics and logs across various instances of services to detect outliers in the instance population based on key performance indicators. The Splunk navigation UI interprets logs to offer more guidance to users, with AI/ML capabilities to troubleshoot and recommend root causes without any need for context switching across different infrastructure monitoring, APM, and log management tools. These solutions add flexibility by enabling any user within the organization to become an observability power user. The many integrations in and out of the solution enable an organization to align Splunk with its existing processes and methods.

Splunk's superior rating on the ecosystem criterion indicates the breadth of training, certifications, and documentation available, as well as a partner program with over 2,000 customer success and service partners.

Splunk user groups are independently created, and Splunk-supported groups hold

events where users of all levels can share technical details of their use cases, stories, difficulties, successes, and mindshare.

Strengths

In terms of the key features, Splunk mostly earns superior ratings, with the exception of predictive analysis getting only an average score. Dashboards are provided in a low-code environment with a consistent UI across all features. RUM, traces, and synthetics are well supported, though volume usage must be kept in mind to control costs. Splunk supports the major public clouds and private clouds with either Splunk Cloud or Splunk Enterprise. Tagging data is handled during collection with OpenTelemetry or manually via an uncomplicated interface. Pushing data with API integration is also a strong area, with a number of integrations available out of the box.

Challenges

With regard to identifying ghost change, Splunk can see infrastructure and topology changes but not software and other configuration changes. Deployment of Splunk Enterprise can become complicated if log sources are spread across disparate locations or business units. Controlling cost can be a challenge, though Splunk does provide tools to help mitigate this.

Purchase Considerations

Splunk Cloud provides predictable and scalable pricing control, earning it a superior rating. It can be purchased in bundles or individually via host-based or volume-based pricing. Similarly, Splunk Enterprise offers pricing that is based either on workloads or volume. All pricing options include support plans.

Splunk Observability Cloud's host-based pricing offers three pricing bundles as well as individual offerings (such as infrastructure monitoring or APM). Each edition of the product bundle scales to include products based on the use case. Volume-based pricing is based on the volume of data ingested. This is also offered for telemetry data such as logs, metric time series, and traces analyzed per minute.

Workload pricing is based on the compute capacity or resources consumed for different search and analytic workloads and includes controls to optimize workloads. The workloads are measured in the cloud using Splunk Virtual Compute (SVC) and customer-managed workloads using virtual CPUs (vCPUs). Activities requiring compute resources include investigating, monitoring, ML, data streaming, indexing, and processing. For customers adhering to specific budgets, multiyear pooled capacity subscriptions and enterprise license agreements (ELAs) enable the use of multiple products with annual rollover. To optimize data usage and storage, users can select low-value but medium- to high-volume data, then filter, enrich, and route it to lower-cost storage.

Splunk Cloud is especially easy to use and deploy for smaller organizations. Splunk Enterprise Security can be added to the Splunk Platform, and the additional cost should be considered to better secure the enterprise. Additionally, many customers leverage Splunk ITSI, which is a fully integrated, premium app built on top of the Splunk Platform that offers AIOps and provides centralized event analytics and correlation for alert noise reduction, anomaly detection, predictive

analytics, business service monitoring, and automation. Splunk is a significant player in the observability space with good cloud and on-premises offerings. Prospective buyers of any size should compare them to other leaders when they consider their shortlist of vendors.

Splunk primarily markets to larger enterprises with additional security needs, a space for which it has significant tooling. Splunk has vertical market support in aerospace and defense, energy and utilities, financial services, healthcare, higher education, and the public sector.

Radar Chart Overview

Splunk is a Fast Mover due to its consistent monthly release schedule. The vendor is positioned as a Leader in the Innovation/Platform Play quadrant due to its significant enhancements across the breadth of its offerings, which can only be skimmed in this review.

StackState

Solution Overview

StackState is a single-platform SaaS offering that can be deployed to any public cloud provider and run as a self-hosted solution on-premises, air-gapped, or as a hybrid combination of all. StackState is based on open standards. It supports all OpenTelemetry MELT and actively contributes to the standard.

StackState has a superior dashboard and reporting system with a suite of out-of-the-box templates and a no-code environment for customizing and sharing dashboards. The product emphasizes the practical application and analysis of the data rather than the ingestion process. The option to integrate with Grafana's visualization system exists if needed.

Though StackState does not have RUM capabilities or synthetic transactions, it handles all OpenTelemetry traces well with customization that can use both low-code and pro-code approaches. StackState is technology-agnostic, offering full end-to-end observability capabilities across the IT environment. It integrates traditional infrastructure with modern cloud environments. Air-gapped private gardens are also supported. However, it gets a poor score for LLM support: StackState is currently investigating, with the help of its clients, what to do about LLMs.

Features for pushing and tagging data are capable because metadata from OpenTelemetry can be ingested, while StackPacks allow add-ons and extensions to push data. Predictive analysis and forecasting are supported with an included Health Forecast StackPack to get on-demand forecasts for the health of any component over the next 12 hours.

The StackState Agent fully supports running in edge environments, based on an instance of SUSE Rancher's RKE2. StackState can't check for ghost changes, but its open source roots may enable this sooner rather than later. Integration with existing CMDBs may allow some ghost change capabilities but would require pro-code additions to Stackstate.

Deployment of the SaaS offering can be fully automated. A single Helm chart installation is required to begin streaming data. Self-service StackState can be installed on a Kubernetes or OpenShift cluster using the Helm charts. Add-ons extend the functionality of StackState, and integrations allow deep connections with external services. Add-ons or extensions may come with a companion integration that translates data from the external system to a format StackState understands. Integrations are currently limited, but the list is expanding. Taken together, these abilities provide for a superior deployment experience.

StackState is very easy to use and provides guided remediation to assist in issue resolution. Remediation guides can be extended or modified to make them specific to an environment. There are four perspectives in the StackState UI relating to the topology under investigation: topology for components and relationships, events for alerts and changes, metrics for telemetry streams, and traces. Time Travel is an innovative StackState feature for troubleshooting from all perspectives. It allows users to travel back in time to the topology state at a specific point in the past. This feature helps engineering teams in post-mortem analysis, allowing them to step through time to reconstruct how an incident evolved.

StackState takes a dual pathway to accessibility and customization with both no-code and pro-code approaches. Most users can access all of StackState's capabilities through a no-code interface, managing configurations entirely via the UI. For those familiar with GitOps methodologies, StackState advocates the use of the StackState CLI, which allows management using modern development practices, catering to those with a more technical, hands-on approach. This dual-path strategy enhances the solution's flexibility, giving agility a superior score.

Strengths

StackState provides two paths for usage: one for nontechnical users and another for developers. This approach allows developers to use methods they are familiar with while giving ITOps users the friendly interface they need. Strengths in dashboards, multicloud functions, deployment ease, and ease of use all work together to give developers observability tools without disrupting their workflow, or at least not too much. The remediation guides allow easier troubleshooting and knowledge capture. The ability to step back in time using the topology model supports better post-mortem analysis.

Challenges

StackState has accepted that LLMs will change the observability landscape but has not determined how LLMs will manifest in their product.

Purchase Considerations

StackState offers good training, solid documentation, and professional services. Community support and a partner system are on the roadmap for the next 18 to 24 months.

The licensing model for StackState is based on per-node monthly billing. The company offers subscription-based pricing without perpetual licenses. The cost is predictable based on the number of nodes in the enterprise. Pricing varies with

the edition selected and the number of nodes. Volume discounts are available for environments with over 250 nodes.

StackState aims to give developers observability tools while keeping the interface usable for ITOps. These considerations should influence those looking at a fast-moving vendor they can grow with and nudge in directions they want to see.

StackState targets SMBs, larger enterprises, and MSPs. In particular, it emphasizes internal teams rather than industry segments: ITOps teams for proactive issue management and system uptime, DevOps teams for continuous monitoring for improved software delivery, and SREs for reliability management and incident resolution. Cloud migrations, hybrid, and multiple cloud environments are also targets to support the organization as a single entity.

Radar Chart Overview

StackState is positioned in the Innovation/Feature Play quadrant. It's an innovative, feature-driven organization offering distinct modes for users and developers, health forecasting, and simple deployment. Due to lower scores for some of the decision criteria we evaluated, it's classified as a Challenger. But it is pushing the boundaries: it has a four-week update process that includes self-hosted implementations, which is unusual in the marketplace. This yields them an Outperformer ranking with expectations of significant future enhancements.

Sumo Logic

Solution Overview

Sumo Logic was built originally as a log management, big data analytics, and SIEM solution, but the company eventually added tracing and metrics to revamp the product into a full observability platform. Sumo Logic is a cloud-native, multitenant SaaS solution hosted on AWS and available in multiple regions. Some features are native to or function only on AWS.

Sumo Logic supports open standards for data collection, such as Telegraf for metrics and OpenTelemetry for tracing, as well as others like Prometheus, FluentD, and FluentBit for other types of telemetry, and legacy open standards from the CNCF. Sumo Logic has a root cause explorer (RCE) to support troubleshooting and root cause isolation in apps and microservices running on AWS, public cloud hosts, and Kubernetes.

Sumo Logic dashboards can display data in two modes. In Basic Mode (a no-code environment), users construct queries by selecting metadata fields, dimensions, metrics, and operators from pull-down lists. With Advanced Mode (a low-code/pro-code environment), users can enter the entire query manually. Advanced Mode will also prompt with pull-down lists of metadata fields, dimensions, metrics, and operators. Dashboards can be shared and pinned as favorites.

Sumo Logic does not support synthetic transactions directly but through CatchPoint, an additional cost integration. The solution uses OpenTelemetry traces but not application-level RUM; Sumo Logic documentation and marketing materials equate OpenTelemetry traces with RUM, which is not entirely accurate. Overall, user interaction performance is below average.

Sumo Logic ingests logs from Google Cloud Vertex as part of its LLM strategy. ChatGPT can be integrated into the SOAR application dashboard but is not connected to any data from Sumo Logic. It is a bare-bones OpenAI connection, and customers must supply their own OpenAI API key. The LLM solution is not directly connected to Sumo Logic data via summarization or other means. When compared to LLMs in the rest of the cloud observability landscape, this key feature is also below average.

Tags (metadata) can be pulled from any data source and defined in Sumo Logic. Pushing is handled through API integration. Prediction works only on log data and will not forecast more than 100 points into the future. A timeline setting determines whether the 100 points are minutes, hours, or days. The amount of historical data available and the algorithm chosen determines the accuracy of the forecast.

Sumo Logic earns a poor score for identifying ghost changes and an average rating for edge observability, as edge observability can be accomplished with installed collectors. Synthetic transactions are the normal edge observability entry point, but Sumo Logic does not have native synthetic transactions. Instead, it relies on integration with CatchPoint, which does not support on-premises private locations.

Sumo Logic succeeds with decent scores for all business criteria. Its observability solution is a cloud-native deployment only on AWS. All other clouds are included through integration apps supplied by Sumo Logic. Many integration applications (particularly for AWS) allow a no-code connection to data sources. However, much of the current documentation does not match marketing materials in this area. The added complexity of determining what is possible without Sumo Logic's help is a problem.

The interface is consistent and easy to use. As noted, dashboards are created via low-code or no-code approaches, but many other areas require pro-code skills, particularly for administration and setup. Agility is weak when connecting to public clouds other than AWS. Integration apps define what can and can't be done, and users need pro-code skills to write integrations. Within AWS, everything works as advertised, but when Sumo Logic is used outside of AWS, it's less straightforward. Data retrieved from other public clouds using Sumo Logic integration apps is usually limited to logs, though these are handled well.

Strengths

Sumo Logic has a robust predictive analytics capability for log data. Its dashboards are another strong area, with basic and advanced modes usable by no-code, low-code, and pro-code users. The Sumo Logic ecosystem is complete and supportive, though the independent forum appears to be inactive. Tagging and pushing metadata is functional using OpenTelemetry to retrieve tag information. Ease of use for users is good, but administration is complex. Sumo Logic focuses on native integration with AWS and is very good at working with log files.

Challenges

Documentation and marketing materials do not adequately describe the features and capabilities of Sumo Logic. The disparity creates a situation where what

customers might expect to do and what can actually be done do not agree. LLM support lacks integration with Sumo Logic other than a UI button directly connecting to OpenAI. Businesses must provide their own API key to enable the functionality. Native functionality is only with AWS, relegating other public clouds to integration apps that generally only retrieve log data.

Purchase Considerations

Sumo Logic provides documentation, training, certifications, and a Sumo Logic-hosted community forum. An independent Reddit subreddit for users also exists.

Sumo Logic is marketed toward organizations of any size. Licensing is available in three tiers: Free, Essentials, and Enterprise Suite. Different features have different credit values that can be applied to usage. A credit is a unit of measure that tracks use, whether data ingested, storage, or metrics, throughout a contract period. Credits can be used as needed, and Sumo Logic continuously tracks credit utilization.

The complexity and difficulties associated with using Sumo Logic outside of AWS means Sumo Logic works best when used exclusively in AWS. If log files from other clouds are sufficient to monitor and understand data outside AWS, then Sumo Logic may be worth a look.

Radar Chart Overview

Sumo Logic is positioned in the Innovation/Platform Play quadrant. It's a platform player with observability products and SIEM and SOAR offerings. Although Sumo Logic has existed since 2010, it's more innovative than it is mature, placing it in the Innovation half.

6. Analyst's Outlook

The cloud observability marketplace has evolved since our last report. The 2023 Radar showed a more stable and simple-to-understand vendor landscape, but that's not the case anymore. Even the biggest players in this space—Cisco, Datadog, Dynatrace, New Relic, and Splunk—have been scrambling to keep up as demand for a more straightforward and comprehensive solution increases. The volume of traffic and logs and the general complexity that enterprises deal with is greater than ever—and continues to grow. Ongoing moves toward digital experiences generate ever more data and complexity.

On top of that, there continues to be confusion about the meaning of observability, which, to us, is relatively clear: its purpose is to make sense out of the glut of monitoring information now available. The questions for which we are seeking answers are important to running modern enterprises efficiently and safely, but no individual person or team can keep an eye on every aspect of a modern IT infrastructure and make sense of what is actually happening. Monitoring answers the questions of on or off, running or not running, fully functional or out of resources, among others. The problem is IT has to monitor *everything*, and monitoring all that data requires tools to help. Good observability tools ask the next-level questions: how can we keep track of all that information? What can we automate, and how can we automate it?

Within this Radar, the table stakes have grown to include APM, cloud resource utilization, and OpenTelemetry. Cloud observability tools with better connections to the DevOps process and a simpler footprint are entering and challenging the marketplace leaders by focusing on specific areas within observability. Chronosphere, Honeycomb, and StackState have placed more focus on developers and their impact on business operations.

Meanwhile, standards like OpenTelemetry and Prometheus have allowed Elastic and Grafana to improve their products without losing their focus on openness and community. The mega-platforms—BMC, Broadcom, IBM, OpenText, and ServiceNow—are challenging the Leaders by bringing a broader range of resources to the table. CloudFabrix barges into the cloud observability world for the first time, expanding what can be done with an RDA pipeline by adding more intelligence. Cloud providers have their own observability tools: AWS and Microsoft have impressive offerings within their very significant worlds.

At the beginning of this Radar, we defined operational intelligence as a process starting with monitoring, growing to observability, and then adding intelligence, which is the ability to infer the operational state of the entire company from observability data.

Generative AI is the keystone bridging observability and intelligence—and in this Radar it's the 10-ton rock dropped in the cloud observability pond. Generative AI is creating a wave of new capabilities that help tame monitoring noise and hint at a promising future where organizations gain operational intelligence about the business as a whole, not just IT.

At present, most vendors are still testing the waters in an attempt to understand what LLMs will mean to them and their customers. However, enterprises looking at the cloud observability marketplace *should absolutely* investigate what a vendor is doing or planning with LLMs as this technology will only become more important in the future.

Prospective customers should complete the following steps as part of their evaluation:

- Understand where you are in your journey to become an intelligent business. You can't get there immediately. Are you still focused on monitoring? Are you taking on a partial or holistic observability approach? Or do you have a strong-but-improving observability practice and need a solution for intelligently adapting that to cross-business enlightenment?
- Develop a picture of your path to improvement from monitoring to observability to intelligence and determine who you want to travel with. Look carefully at the vendors in this Radar and evaluate where they are on the journey to intelligence—you'll be a partner on this journey.
- Finally, to set yourself up for success, plug the remaining holes in your processes and, if you have an incumbent partner, work with them to guide their products. The ecosystem of each vendor is reviewed here. That ecosystem will be critical in determining what vendors do with LLMs.

Observability brought the promise of automation to the table in a meaningful way. However, not all vendors have embraced it yet. Service orchestration and automation suppliers have begun adding observability to their tools. Cloud observability should take notice, but not try to boil the ocean. What can be automated within cloud observability will be the focus for the next iteration of this report, along with what to do about ChatGPT and other LLMs.

To learn about related topics in this space, check out the following GigaOm Radar reports:

- [GigaOm Radar for Network Observability](#)
- [GigaOm Radar for Kubernetes Resource Management](#)
- [GigaOm Radar for Application Performance Management](#)

7. Methodology

*Vendors marked with an asterisk did not participate in our research process for the Radar report, and their capsules and scoring were compiled via desk research.

For more information about our research process for Key Criteria and Radar reports, please visit our [Methodology](#).

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 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.

10. Copyright

© [Knowingly, Inc.](#) 2024 "*GigaOm Radar for Cloud Observability*" is a trademark of [Knowingly, Inc.](#) For permission to reproduce this report, please contact sales@gigaom.com.

GIGAOM

Knowingly Corporation

3905 State Street #7-448

Santa Barbara, CA 93105-5107

[Subscribe to our monthly analyst insights newsletter](#)

Stay on top of emerging trends by joining our newsletter, a monthly publication from our leading network of analysts.

[SUBSCRIBE NOW](#)

Research

- > Methodology
- > Vendor Escalation Policy
- > Research Calendar
- > Analyst Videos
- > AI, Data & Analytics
- > Security & Risk
- > Cloud, Infrastructure & Management
- > DevOps
- > Network & Edge
- > People, Processes, & Applications
- > View All Research

For Vendors

- > Customer Centric Enablement and Activation
- > Total Cost of Ownership & Engineering Benchmarks
- > Radars
- > Key Criteria
- > Advisory Services
- > Enterprise Subscription
- > Value Engineering
- > Vendor Marketing Content Review

Insights

- > Case Studies
- > Blog
- > Press Room

Company

> [Why GigaOm](#)

> [Our Team](#)

> [Partners](#)

> [Careers](#)

> [Contact us](#)



[Privacy Policy](#)

[MSA](#)

[Terms of Service](#)

[Code of Conduct](#)

© GigaOm

All Rights Reserved 2024