

Attribute / Feature	New Relic	Datadog	Splunk Observability	Elastic Observability	Grafana Cloud (with Prometheus, Loki and Tempo)	ServiceNow (Formerly Lightstep)	AppDynamics	Dynatrace	AWS-native Observability
Website URL	https://newrelic.com/	https://datadoghq.com/	https://www.splunk.com/	https://www.elastic.co/	https://grafana.com/	https://www.servicenow.com/products/observability.html	https://www.appdynamics.com/	https://www.dynatrace.com/	
Gartner Magic Quadrant	Leader	Leader	Leader	Visionary	Visionary	Visionary	Challenger	Leader	Challenger
Deployment Model	SaaS	SaaS	SaaS, On-prem	SaaS, On-prem	SaaS, On-prem	Implemented as SaaS, but uses local or cloud-based microsatellites that bridge the monitored components and Lightstep platform.	SaaS, On-prem	SaaS, On-prem	SaaS
Ease of Use	Moderate	Moderate	Difficult	Difficult	Difficult	Moderate	Moderate	Moderate	Easy to start, but can be difficult and complicated depending on your specific use case.
Agent based	Yes, Installed on hosts and/or within applications	Yes, you can install and configure the Datadog Agent on a variety of platforms, including Linux, Windows, macOS, Docker, and Kubernetes.	Uses a combination of agents, forwarders, indexers and search heads to collect data from monitored components. If you need to collect comprehensive and reliable data from a large number of devices, then agents are the best option. if you are concerned about overhead or security, then you may want to consider agentless data collection methods.	You can use a combination of agent-based and agentless integrations to collect the data you need to monitor your environment. Some Elastic Observability agents include: APM, Infrastructure, RUM and synthetic monitoring agent	Open source agents runs on monitored devices and collects metrics, logs and traces.	Uses OpenTelemetry launchers, Jaeger agents or Zipkin to collect telemetry data, which is then fed to the microsatellites that communicate with the platform.	Yes	Yes. OneAgent is installed on each host, and it automatically discovers and instruments all of the applications and services running on that host.	No, integrates natively with AWS services to collect metrics, logs, and traces.
Log Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Infrastructure Monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud Observability	Cloud, hybrid, multi-cloud and edge environments	Cloud, hybrid, multi-cloud, and edge environments.	Cloud, hybrid, multi-cloud, and edge environments.	Cloud, hybrid, multi-cloud, and edge environments.	Cloud, hybrid, multi-cloud, and edge environments.	Cloud, hybrid, multi-cloud, and edge environments.	Cloud, hybrid, multi-cloud, and edge environments.	Cloud, hybrid, multi-cloud, and edge environments.	AWS only
Microservices Monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Kubernetes Monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, provides robust tools and integrations for monitoring Kubernetes clusters, with special capabilities and optimizations for Amazon EKS and Fargate.
Serverless Monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
APM	Yes	Yes	Yes	Yes	Yes, Tempo is a highly scalable and cost-effective tracing system that is compatible with OpenTelemetry, Zipkin, and Jaeger.	Yes	Yes	Yes	Yes, its suite of services like AWS X-Ray, Amazon CloudWatch, and integrations with third-party tools collectively provide robust APM functionalities.

Real User Monitoring	Yes, browser monitoring implies that it has the capability to perform Real User Monitoring, providing insights into how real users are interacting with web applications and where improvements can be made to enhance the user experience.	Yes, Datadog RUM collects data from a variety of sources, including: -Browser JavaScript -Server logs:	Yes, Splunk RUM provides real-time, front-end user monitoring and troubleshooting. It collects and analyzes metrics and traces from users' browsers to give you visibility into the performance of your web and mobile applications.	Yes, quantify and analyze the perceived performance of your web application with User Experience data	Yes, It includes a highly configurable web SDK for RUM that instruments browser frontend applications to capture observability signals.	Yes	Yes, it collects data on metrics such as page load times, JavaScript execution times, and user interactions.	Yes, Dynatrace RUM provides insights into the end-user experience of your web and mobile applications. It collects data on user actions, page load times, and other performance metrics.	No. It lacks a dedicated Real User Monitoring solution.
Synthetic Monitoring	Yes, the platform provides tools for creating and managing synthetic tests to monitor and evaluate the performance, availability, and reliability of web applications and services	Yes	Yes, Splunk Synthetic Monitoring provides full-featured synthetic monitoring and web optimization. It allows you to create and run synthetic tests to monitor the uptime, performance, and functionality of your web and mobile applications.	Yes	Yes, powered by k6, a leading open source load testing tool. k6 can be used to generate realistic traffic to your applications and infrastructure at scale.	Yes	Yes	Yes	AWS provides tools for implementing synthetic monitoring, particularly through AWS CloudWatch Synthetics, Lambda functions and health-checking to achieve the same function.
Anomaly Detection	Leverages machine learning algorithms and statistical techniques to automatically detect and alert on unusual patterns in the monitored data. The "applied intelligence" aspect suggests that the platform not only identifies anomalies but also provides insights or recommendations based on these detections, aiding in quicker diagnosis and more effective response to potential issues.	Datadog anomaly detection uses a variety of techniques to identify anomalies, including statistical analysis and machine learning.	Offers a number of features that make it well-suited for detecting anomalies in time-series data, like automatic seasonality detection, and a number of statistical, machine learning algorithms and rule-based methods.	Yes, utilizes automated, real-time and customizable anomaly detection rules.	Grafana Cloud's anomaly detection features are powered by its machine learning engine. This engine can be used to train models on your historical data to learn what normal behavior looks like. Once a model has been trained, it can be used to identify anomalous data points in real time.	Yes	Yes, both ML and rules based detection	Yes, both ML and rules based detection	AWS offers a comprehensive set of tools for anomaly detection, leveraging machine learning and pattern recognition across a wide range of applications.
Alerting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integration Capabilities	Integrates with more than 470 third-party technologies	Built-in support for more than 500 third-party integrations	Supports more than 2,400 Splunkbase apps and add-ons, and can ingest telemetry data from across the entire technology landscape	There are currently over 250 supported 3rd party integrations.	There is no published total integrations supported. Here's the list of integration references: https://grafana.com/docs/grafana-cloud/monitor-infrastructure/integrations/integration-reference/	There are over 600 supported third-party integrations.	There are over 190 supported 3rd party integrations. These integrations cover a wide range of technologies.	Supports more than 600 third-party technologies and is built on open standards	Provide deep integration AWS services, however, Cloudwatch can monitor and log data from non-AWS sources, but will require additional configuration. Xray can also trace requests starting from on-prem or other cloud environments using SDKs. Can also send data to 3rd party tools like Grafana, Splunk and Datadog.
Vulnerability Detection	Yes	Yes	Allows integration with vulnerability detection tools and enrich these data with asset context, severity and remediation recommendations.	Yes	Grafana Cloud's vulnerability detection features are powered by the OSV Scanner, an open source vulnerability scanner	Yes, it provides a number of anomaly detection features, including: -Statistical -Machine learning -Correlation analysis	Using integrations with vulnerability scanners, AppDynamics provides a unified view of vulnerabilities across all environments	Dynatrace Runtime Vulnerability Analytics (RVA) detects and analyzes vulnerabilities in real time across all layers of your application stack. It includes SCA, DAST and open source dependency scanning.	AWS offers a range of services for vulnerability detection, focusing on different aspects of security and compliance.

Incident Management	Yes, in the context of IT and application monitoring involves the identification, analysis, and response to incidents that affect the performance and reliability of IT services. Often, monitoring tools integrate with platforms like Slack, PagerDuty, and others for efficient communication during incident response.	Yes, provides a centralized view of all of your incidents, and it gives you the tools you need to collaborate with other team members to resolve them quickly.	Yes, Splunk On-Call provides automated incident response. It helps you to streamline your incident management process and reduce the time it takes to resolve incidents.	Yes, using features such as case management and collaboration tools allows you to receive alerts, investigate incidents and coordinate response effectively.	Grafana Cloud IRM provides a unified platform for incident response and management. It includes features such as: -Incident declaration and tracking -Incident response teams and roles -Incident communication and collaboration -Incident playbooks and runbooks -Incident reporting and analysis	Yes, its capabilities help you to identify, prioritize, and resolve incidents quickly and efficiently.	Through integrations with a number of ITSM tools to help organizations manage incidents.	Dynatrace Security Analytics provides a single pane of glass for incident management. It integrates security data with observability data to give you a complete view of your security posture. Dynatrace Security Analytics also includes a number of features to help you manage incidents	AWS provides a comprehensive set of tools for managing incidents, from detection and alerting to investigation and resolution. These tools, along with integrations with popular third-party incident management solutions, enable organizations to effectively manage and respond to incidents in their AWS environments.
Dashboards and Visualizations	Known for its flexible and customizable monitoring capabilities, so users can often tailor dashboards and visualizations to fit their specific monitoring requirements.	Provides out-of-the-box and allows you to create your own custom dashboards and visualizations.	Wide range of dashboards, including cloud observability, microservices and serverless observability, anomaly detection, and vulnerability detection. Also allows you to create custom dashboards and visualizations	Provides out-of-the-box and allows you to create your own custom dashboards and visualizations.	Grafana Cloud offers a wide range of dashboards and visualizations that can be used to monitor your applications, infrastructure, security, and SLAs.	ServiceNow Cloud Observability provides a variety of pre-built dashboards and visualizations, as well as the ability to create custom dashboards and visualizations.	Comprehensive list of pre-built dashboards and visualizations. It also allow users to create custom dashboards and reports.	Dynatrace offers a variety of dashboards and visualizations that you can use to monitor and analyze your applications and infrastructure. It also allow users to create custom dashboards and reports.	AWS offers a broad range of dashboard options for observability, catering to various aspects of cloud resource monitoring, application performance, security, IoT, and business intelligence.
OpenTelemetry Support	Yes	Yes, it supports the OpenTelemetry Protocol (OTLP) and exporter	Yes, offers a number of features and integrations that make it easy to use OpenTelemetry	Provides native support for the OpenTelemetry protocol (OTLP) to ingest traces, metrics, and logs.	Yes, to use Grafana Cloud with OpenTelemetry, you can use the Grafana Agent or the OpenTelemetry Collector.	Yes	Yes	Yes, Dynatrace provides a number of ways to ingest OpenTelemetry data, including: -Via OTLP -Via OTLP collector -Via OTLP exporter -Via AWS Distro	Yes, particularly through AWS Distro
Customization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pricing Plans	Free, Standard, Pro and Enterprise. You are charged based on the amount of data you ingest and the number of billable users you have.	Free, Pro and Enterprise. Your price will be determined by: -Amount of data ingested -Number of hosts monitored -Add-ons used	Contact Splunk directly for details about Splunk Cloud Platform and Splunk Enterprise licensing plans. Plans vary for the individual products.	Basic, Gold, Platinum and Enterprise. You can add features, such as ML, anomaly detection and alerting on pay-as-you-go.	Available in 4 subscription plans: Free, Pro, Advanced and Enterprise Stack plans	Offers three subscription plans: Essentials, Standard and Premium. Community version has been discontinued in 2023. Pricing is based on the number of hosts, containers, and services that you monitor. The price per host, container, or service varies depending on the pricing plan that you choose. There are additional charges for certain features, such as anomaly detection and synthetic monitoring	AppDynamics offers three pricing plans: -Starter -Standard -Enterprise These are based on the number of AI's (Application Instances) which could correlate to node count and user count depending on how it is architected and deployed.	Comes with subscription and pay-as-you-go plans. On both plans, a tiered GiB model is used in a diminishing cost per GiB as volume increases. A GiB hour is a unit of measurement that is used to quantify the amount of data that is ingested by Dynatrace. It is calculated by multiplying the amount of data that is ingested by the amount of time that the data is ingested for.	Pricing for AWS services can be estimated using this calculator: https://calculator.aws/ . There may be additional costs based on factors like data transfer, API calls, and other AWS services used in conjunction with these observability tools.