Cool Vendors in Monitoring and Observability — Modernize Legacy, Prepare for Tomorrow

By Padraig Byrne, Gregg Siegfried, Venkat Rayapudi
Observability continues to increase in importance as a key mechanism to understand modern architectures and applications. Legacy monitoring solutions may not innovate with sufficient speed, so I&O leaders should look to these cool vendors to close their visibility gaps.

**Additional Perspectives**
- Summary Translation: Cool Vendors in Monitoring and Observability — Modernize Legacy, Prepare for Tomorrow (11 February 2022)

**Overview**

**Key Findings**
- Observability in modern environments results in accumulation of large data volumes at high velocity, thereby increasing the challenge of quickly finding the important “needles in the haystack.”
- Troubleshooting microservices systems continues to be problematic due to their highly distributed and ephemeral nature.
- Distinctions between IT operations and development teams are rapidly diminishing, and legacy monitoring tools are not designed to operate as part of a DevOps value stream.

**Recommendations**

I&O leaders responsible for monitoring and observability should:
- Troubleshoot more effectively by implementing observability tools that support the efficient analysis of high-cardinality data.
Increase visibility by adopting platform-aware tools that support the complete service delivery environment. Cloud and cloud-native platforms such as Kubernetes generate telemetry that can be instrumental in identifying unknown unknowns.

Observe the full life cycle of your services by including build, test, deploy and release instrumentation. This "shifting left" supports traceability, which is becoming a critical part of the diagnostic workflow.

**Analysis**

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

**What You Need to Know**

As noted in Hype Cycle for Monitoring, Observability and Cloud Operations, 2021, the term observability has become ubiquitous, and 2021 is shaping up to be "the year of observability." Although it continues in many cases to be used (or misused) as synonymous with monitoring, organizations are finding that observability thinking provides new solutions to modern problems.

Many early definitions of the term focused on the different ways to ingest telemetry from a system — metrics, logs and traces being the so-called three pillars of observability — but it has expanded to encompass much more.
In this document, we look at four vendors that are expanding capabilities around four areas related to observability:

- **Cribl** allows organizations to efficiently manage large datasets generated by observability systems.
- **Komodor** focuses on capturing and correlating changes in Kubernetes environments.
- **Observe** supports the exploration of event data through relationships and temporal analytics.
- **Rookout** provides observability in production systems, allowing developers and SREs access to real-time information about application performance.

In this report, we also look back at two previous Cool Vendors in the domain of observability — Epsagon and Lightstep — who have both been acquired in recent months.
Cribl
San Francisco, California, U.S. (cribl.io)

Analysis by Venkat Rayapudi

Why Cool: Cribl's LogStream provides a controlled abstraction layer for managing log stream pipelines connecting multiple sources with multiple destinations. It offers advanced routing logic with a low-code interface with the ability to visualize the log data flows.

LogStream provides native integration for streaming data with flexibility into major log monitoring solutions, public cloud object storage, and APMs such as Splunk, Amazon S3 and Datadog. It inherently understands the different protocols and packages required for data transfer.

Although major log monitoring solutions offer log aggregation components, they are hard to configure, do not provide any visibility into data flows and are not designed for reducing log monitoring licensing cost. With Cribl's LogStream, log data can be enriched with context information, such as geoIP, for downstream analysis based on the organization's security and compliance requirements. It offers an easy-to-use interface to configure routes and provides out-of-the-box packs for parsing and data manipulation use cases. This enables the organization to stream log data to multiple destinations based on the metadata and routing logic defined. Because the routing logic is applied before ingestion, it aids in reducing licensing costs.

Log aggregation software is typically tied with the log ingestion technology. When organizations switch providers, they end up replacing log aggregation software and configuration as well. Cribl's LogStream enables portability for log collection with a vendor-agnostic approach to switch log monitoring providers with a simple configuration without needing to install additional software. Cribl LogStream also offers visual data flows in a pipeline model with an appealing UI interface that is absent in typical log aggregation softwares. LogStream offers both self-hosted and SaaS deployment models including free tiers.
Challenges: Being a fairly new startup, Cribl lacks brand awareness in this nascent log aggregation and data enrichment space. Organizations need to work on building a convincing business case for Cribl because it will be a net new investment, although it may reduce overall total cost of ownership in the long term. With Cribl's SaaS offering being fairly new, the hosting cloud provider options and regions are limited and continue to expand over time.

Who Should Care:

- IT operations and SREs that are responsible for log data enrichment and overall log monitoring strategy as part of monitoring and observability
- Security operations personas that are focused on improving threat intelligence with data optimization/enrichment and managing sensitive information for incident response
- Enterprise procurement teams and those responsible for IT budgets who are looking for ways to reduce their overall spend on IT monitoring and observability

Komodor
Tel Aviv, Israel (https://komodor.com)

Analysis by Gregg Siegfried

Why Cool: Komodor simplifies the troubleshooting of Kubernetes-based workloads by capturing any changes made to cluster configuration or applications and making those changes available to platform operators and site reliability engineers in a way that reduces mean time to repair (MTTR) and facilitates collaborative problem solving. By integrating with today's most common operations tools, such as Slack, Datadog, LaunchDarkly and Grafana, Komodor presents those tasked with troubleshooting anomalies or diagnosing pathologies a comprehensive change history that helps identify root cause and quickly reverse problematic changes.

Deploying Komodor is not an all-or-nothing proposition — the software can be configured to watch or ignore specific resources and namespaces, and even to redact sensitive data before notifications are sent to the Komodor portal. Slack integration enables the tool to be used directly from the Slack client itself, which maintains focus and enhances collaboration.
Challenges: A cluster-centric perspective on change may not be ideal for applications that span clusters or complete enough for those that operate in a hybrid mode where portions execute outside of Kubernetes. An increased emphasis on the use of change data in operations tools recently has stiffened the competition in the functional area that is Komodor's focus.

Who Should Care: Platform operations teams responsible for the health and performance of Kubernetes clusters and the site reliability engineers and product teams that build and deploy applications on Kubernetes are the primary audiences for Komodor. Organizations that are moving workloads to Kubernetes from other platforms can accelerate the learning curve by understanding in detail (through Komodor's Kubernetes diff) the impact of deployments and cluster configuration changes.

Observe

Analysis by Gregg Siegfried

Why Cool: Helicopters have been described as thousands of parts flying in close formation, and this metaphor may also apply to modern applications and platforms — perhaps for various values of “close.” The relationships between the parts is often where the interesting things take place, and many of our diagnostic tools focus too much on the parts themselves rather than these relationships. Observe has created a SaaS-based solution that supports the ingestion and transformation of high-volume telemetry, as well as interactive analysis, exploration and alerting based on conditions uncovered or detected in the resources or their associations.

Powered by the Snowflake Cloud Data Platform, Observe can be used much like a traditional log analysis tool such as Elasticsearch, and can ingest “anything with a time stamp” — metrics and traces included. Beyond a search-engine-like experience, however, this ability to create “things” (resources) out of your machine data, curate a graph of associations between them and track their state over time distinguishes Observe's solution from search or index-based products.

Challenges: Increasing competition in the observability space rewards name recognition and short time-to-value, which is more difficult to demonstrate in a fundamentally novel solution like Observe. Although support for Kubernetes and AWS is well established, additional integrations are being created based on demand. This may lengthen time-to-value for customers intending to leverage the product in other platforms.
Who Should Care: Organizations that have adopted modern platforms and application architectures that are challenged by problem identification and incident analysis will benefit from Observe's capabilities. In addition, if the cost or operational overhead of your existing monitoring and observability tools is problematic, Observe's solution may serve as a more capable and cost-effective alternative. The end-user personas will generally be site reliability engineers, developers and cloud engineers.

Rookout

Analysis by Padraig Byrne

Why Cool: Rookout enhances observability to live production environments by enabling teams to debug actively running code. Rookout allows the use of “nonbreaking breakpoints” to get instant outputs on key variables and metrics from complex, distributed systems including microservices and cloud-native applications. This mechanism allows a nonintrusive way to interact with running applications to aid rapid problem identification and resolution of service-impacting issues, without the need to write more code and redeploy versions of the application.

Rookout allows a polyglot approach with support for Java, .NET, Python, Node.js and Ruby (support for additional languages including Golang is planned). Because it runs against real production data, Rookout puts an emphasis on data security and is compliant with a number of regulations and certifications, including SOC2, GDPR and HIPAA. It can be deployed in either a fully SaaS mode or as a hybrid on-premises/SaaS mode that allows sensitive data to remain within the organization's firewall.

Rookout is also available to Cisco clients under an OEM arrangement as Cisco AppDynamics Deep Code Insights.

Challenges: Rookout is one of a number of vendors in the emerging area of production debugging. Existing APM vendors have some feature overlap and will continue to increase their features in this space. Additionally, hyperscalers such as AWS and Azure continue to build out their observability tools for microservices, which may in the future become more attractive than third-party tools.

Also, because Rookout operates in live environments, care must be taken with the design and implementation of the tool because it could provide access to sensitive and regulated customer data.
Who Should Care: Rookout will be of interest to a number of teams, including developers, SREs and IT operations. Any role that involves responsibility for the operation of complex applications in modern cloud environments, and for the resolution of any issues that arise, should assess Rookout for its applications.

Rookout is also of interest to engineering managers looking to improve the productivity and velocity of their development teams by reducing time spent on traditional logging, debugging and reproducing issues for remediation.

Where Are They Now?

Epsagon
San Francisco, California (www.epsagon.com)

Profiled in September 2019

Analysis by Padraig Byrne

Why Cool Then: In 2019, observability vendor Epsagon offered a distributed tracing solution focused exclusively on solving the challenges associated with monitoring within microservices and serverless environments. Epsagon aimed to tackle the issues of application scale and complexity when deployed in event-driven distributed environments with its observability platform.

Where Are They Now: In August 2021, Cisco announced its intent to acquire Epsagon and hired key personnel into its team. According to the Cisco press release: “Epsagon will play a key role in expanding and accelerating Cisco’s comprehensive Full-Stack Observability roadmap.”

Who Should Care: Existing Cisco AppDynamics clients should look forward to having greater visibility of their containers and microservices environments.

Lightstep
San Francisco, California (https://lightstep.com)

Profiled in September 2018

Analysis by Padraig Byrne
Why Cool Then: Lightstep was one of the earliest vendors to explicitly target observability as a differentiated market from traditional monitoring. In 2018, we thought that Lightstep was cool because it was an APM-like solution focused on microservices-based applications, using open-source distributed tracing to track transactions across microservices. Its founders included ex-Google engineers who had been among the first to implement distributed tracing as a way to understand complex applications.

Where Are They Now: In May 2021, ServiceNow announced that it had signed an agreement to acquire Lightstep. The acquisition of Lightstep gives ServiceNow a much stronger presence in the monitoring and visibility sector, with which to bolster its DevOps capabilities. ServiceNow has indicated that, contrary to its usual acquisition path, Lightstep will not be replatformed and will retain its brand and direct web sales model. For example, in August 2021, ServiceNow announced Lightstep Incident Response, an automated incident response (AIR) solution using Lightstep branding.

Who Should Care: ServiceNow has a significant presence in the large enterprise market. Many of these companies have started their journey to microservices and cloud-native architecture, and may look to deploy their first observability tools by implementing Lightstep in their environment.

Evidence


2. ServiceNow to Acquire Lightstep, Combining Next-Generation Observability With the World’s Leading Enterprise Digital Workflow Platform, ServiceNow.

Recommended by the Authors

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

Vendor Rating: ServiceNow

Innovation Insight for Observability

Magic Quadrant for Application Performance Monitoring

Monitoring and Observability for Modern Services and Infrastructure
Actionable, objective insight

Position your IT organization for success. Explore these additional complimentary resources and tools for I&O and IT leaders:

**Resource Center**
*Infrastructure & Operations Leaders*
Explore insight, advice and tools to help I&O leaders address their top challenges.

**Roadmap**
*2021-2023 Emerging Technology Roadmap*
Make technology investment decisions with confidence.

**Tool**
*IT Score for I&O*
Evaluate I&O capabilities to drive better business outcomes.

**eBook**
*2022 Leadership Vision for Infrastructure & Operations*
Get a data-driven view of three strategic priorities I&O leaders must action upon.

Already a client?
Get access to even more resources in your client portal. Log In
Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 1 855 811 7593

**International:** +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/it

Stay connected to the latest insights

Attend a Gartner conference
View Conference