REPORT REPRINT

In monitoring, it's about bringing together all the data

MARCH 21 2019

By Nancy Gohring

We are seeing more vendors develop ways to analyze operations data from across the hybrid IT landscape. New requirements, including an awareness of topology and embracing open source are emerging.

Summary

Two years ago, we wrote about vendors developing an approach to monitoring that could be thought of as ITOA 2.0. These vendors were enabling customers to gather data from across their IT environments and run advanced analytics across that data for a variety of use cases, including to quickly understand the root cause of problems and to begin correlating IT performance with business performance.

We have since seen a material advancement of this concept, with new vendors emerging as competitors and with a variety of unique approaches to achieving the vision.

451 TAKE

Traditionally, IT teams used discrete tools to monitor different layers of the application stack – the application, servers, storage, network – with each tool employed by specialists responsible for a piece of the stack. That approach worked well for supporting monolithic applications. Today's applications, however, are distributed and share resources, employ containers and APIs, and run on multiple cloud services, on-premises infrastructure and public networks while interacting with many other components. IT teams require a unified view to better understand the relationship between the components in order to troubleshoot and optimize.

To deliver that unified view, we believe that a vendor must have a number of table-stake capabilities, including being open to a variety of integrations, agnostic about the format of data that's ingested, ability to accommodate large volumes of data and harness advanced analytics techniques including machine learning to generate insights. Vendors also must be able to understand the topology of a user's environment and should allow customers to query the data they collect. We see vendors that are able to do all the above as the most likely to emerge as successful in meeting customer needs.

For the past few years, vendors have been working on approaches to analyzing operations data collected from all components of the stack. Doing so reduces the alert storms that ensue as a cascading set of problems ripples across the components that make up an application. These new products also enable a much quicker or potentially automatic root cause analysis. The four requirements that we identified two years ago remain key to delivering on this vision. They are:

- Openness: Any vendor that is positioning its offering as a central point for analyzing all IT operations data must be open to analyzing data collected by their customers' tools of choice, even if those tools are made by competitors.
- Data agnostic: The more kinds of data these systems can consume, the better intelligence they'll deliver. Some of the products can handle logs, metrics, events, business data and other unstructured types of data.
- Scale and speed: Tools in this category must be able to analyze potentially large volumes of data and do so quickly, in a matter of seconds.
- Advanced analytics: Without harnessing machine learning techniques, vendors are unlikely to be able to deliver the insights their customers require.

As vendors have developed their capabilities in this arena, new requirements and challenges have emerged:

- Topology awareness: In a complex, distributed environment, topology awareness becomes key to identifying when a series of events are related to the same root cause. Vendors use different approaches to gathering topology insight, including by correlating anomalies that occur around the same time. Others may monitor communications to develop a topology. Not all vendors are incorporating topology awareness into their systems and in some cases this omission may make their tools less effective at quelling alert storms and accurately identifying root causes.
- Data centralization approach: Vendors that aim to serve as a central data repository for all IT operations data face a notable challenge: ingesting and storing all data from a third-party tool incurs costs. Passing that cost along to the customer has the effect of requiring the customer to pay for that data twice: once when collected by the third-party tool, and again when ingested into the ITOA 2.0 tool.

We've seen a couple of approaches to try to address this challenge. One is to ingest only events, or another subset of data, into the centralized tool. The downside is that doing so raises the potential of omitting important data sources and thus decreasing the accuracy of insight that the tool can deliver.

Another approach is to stream the data from a third-party tool, storing only incremental data. The approach solves the storage cost problem, but may slow down the process of accessing additional data from the third-party source.

- Openness: We mention above that these tools must be open to analyzing virtually any data, even if it's collected by a competitor. But there's another type of 'open' that's growing in importance: open source software. We're seeing open source tools play a growing role in monitoring environments, as, for instance, Prometheus emerges as a popular tool for monitoring Kubernetes environments, InfluxDB usage grows, Grafana expands into logs, the Elastic Stack continues to gain new users and OpenTracing becomes standard in distributed tracing. Vendors that integrate with or expand on these systems will tap into a large customer base. Vendors that ignore the momentum behind these open source software tools won't remain competitive.
- Querying capabilities: While dashboards, preconfigured and custom, are helpful in many use cases, in complex, dynamic environments, unique problems often require the flexibility to query the available datasets in search of anomalies. We find that sophisticated troubleshooters require and appreciate a flexible and easy-to-use querying capability. While not all end users will need to query or have the experience to do so, we see this as an emerging requirement for a set of users.

In our previous report on ITOA 2.0, we highlighted the following vendors: BMC, CA Technologies, AppDynamics, Datadog, Loom Systems, Rocana, Scalyr, Sumo Logic and Wavefront. Rocana was since acquired by Splunk and Wavefront by VMware. We continue to see these vendors as pursuing the ITOA 2.0 vision. This year we highlight additional vendors that are also active in this space:

- *Dynatrace:* Dynatrace has just begun positioning its product as a platform that businesses can use for integrated APM and infrastructure monitoring as well as front-end monitoring via synthetics and RUM capabilities. One difference between Dynatrace's approach and some others is that it appears to be focusing primarily on collecting data across these systems itself, rather than opening up the ability for customers to ingest data they're already collecting from third-party monitoring tools. While it announced that it is inviting customers to ingest data from third-party tools, its integrations so far are with tools in adjacent categories, like CI/CD tools. We think it's a shortsighted approach not to embrace virtually any data source a customer wants, even if it's collected by a competitive vendor.
- *OpsRamp:* While OpsRamp has its own mechanisms for collecting operations data about infrastructure performance, it also integrates with third-party infrastructure monitoring, APM and log analytics tools. It has been investing in its machine learning capabilities such that it can deliver advanced event analytics and incident management capabilities so that customers can embrace OpsRamp as a central observability tool.

- *ScienceLogic:* ScienceLogic is positioning its SL1 platform as a tool that customers can use to centralize their IT operations data. Key to its offering is ScienceLogic's techniques for contextualizing the data it collects, either via its own methods or from third-party tools, in order to build a granular topology of a customer's environment. SL1 is designed to be a two-way hub, such that customers can easily export the contextualized data to, for instance, a BI tool or a custom-built machine learning engine. We like ScienceLogic's approach to focusing on its core strengths around collecting operations data about a wide variety of infrastructures and building a topology.
- *SignifAI/New Relic:* We think SignifAI, acquired by New Relic in January, brings important capabilities that put New Relic in the position of serving as a central source for collecting and analyzing IT operations data. SignifAI is most often grouped with event analytics competitors. However, SignifAI was built to analyze metrics, logs and events, positioning it to analyze the broad set of operations data required in modern environments in order to aptly reduce alert noise and accurately pinpoint root cause. Combined with the querying and visualization capabilities in New Relic Insights, we think SignifAI boosts New Relic's competitiveness as an ITOA 2.0 tool.
- *Splunk:* In 2018 Splunk rolled out an infrastructure-monitoring product based on a new metrics-collecting back end. Combined with its log management, machine learning capabilities, event analytics and alerting capabilities (via its VictorOps purchase), Splunk can and does serve as a central source of truth in IT operations. It has an extensive and growing library of integrations in order to collect data from the wide array of technologies its customers use.
- *StackState:* StackState's software analyzes metrics, logs, events and other data, including from Google Analytics, social media and CI/CD tools, in order to deliver a broad view of IT systems and to assist teams in discovering the root cause when problems occur. StackState uses the data it collects to learn about dependencies, allowing it to build a topology of a user's IT environment. Customers can use the StackState agent to collect metrics, or they can rely on data collected by third-party monitoring and logging tools that they already have in use. StackState streams data from third-party tools – storing, for instance, only the incremental change when a new version of an application is pushed, thus cutting back on the cost of ingesting and storing all data from other tools.
- *Zenoss:* Zenoss is positioning its new SaaS offering as a central collection and analytics platform for essentially all operations data, including infrastructure monitoring, APM, logs and events. In addition to collecting that array of data from other monitoring vendors, Zenoss is building out its own capabilities with, for instance, a relatively new agent for collecting data, in addition to the long and growing list of infrastructures that it polls for data. For customers that have historically viewed Zenoss as a 'monitor of monitors,' this modern take on that legacy function makes sense.

Conclusion

The vendors best positioned to thrive in this space are those that deliver on all the requirements that we've identified. Some may offer these requirements through partnerships or integrations, in the way that ScienceLogic, for example, has supported data export so that customers can take advantage of third-party machine learning engines. But without insight into topology, support for integrations with third-party monitoring tools and the scale to meet big-data needs, we think vendors will find they can't serve customer needs.

One additional challenge that we anticipate is that in most cases setting up these products as a centralized source for IT operations data is complex. We think that vendors that invest in techniques for simplifying the setup process will be more successful. In addition, this complexity of deployment represents another opportunity for MSPs, which we are seeing increasingly employed by businesses for assistance in cloud migration and the related shift in requirements for monitoring. Setting up and optimizing an ITOA 2.0 tool represents additional opportunity here.