

REPORT REPRINT

StackState tackles monitoring data silos

MARCH 04 2019

By Nancy Gohring

The company joins a host of vendors aiming to solve problems facing organizations that struggle to discover the cause of problems in complex IT environments.

THIS REPORT, LICENSED TO STACKSTATE, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.



Summary

StackState is a young vendor responding to demand from the many organizations that struggle to get a centralized view of application and infrastructure performance in order to quickly discover the cause of performance problems. The company takes a modern approach, open to analyzing data from a variety of sources and investing in further development of its machine-learning capabilities.

451 TAKE

StackState's openness to working with data from a wide range of sources allows customers to stick with the tools they are already invested in. However, the flip side to its approach is that it represents yet another tool at a time when many organizations we talk to are looking to reduce the number they use. We think StackState makes a good acquisition target, with possible suitors including Zenoss, LogicMonitor or ScienceLogic. StackState would deliver a quick boost to any of those vendor's machine-learning skills, although such an acquisition comes with varying degrees of overlapping capabilities.

Context

While working for Xebia as consultants, the company's founders developed the technology behind StackState to solve problems facing the operations team at ING bank. In 2015, Xebia spun off StackState as a separate company designed to commercialize the technology and make it available to other customers. StackState has received \$9m in funding from Xebia.

Based in the Netherlands, StackState is just ramping up, with nine paying customers, most of which signed up in the fourth quarter. It is currently working on raising additional funding.

Products

StackState's software analyzes metrics, logs, events and other data in order to deliver a broad view of IT systems, and to assist teams in discovering the root cause when problems occur. 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 positions its agent primarily as available to fill gaps in what a customer might have.

StackState can ingest data beyond typical monitoring data, including from Google Analytics, social media, business metrics, CMDBs, CI/CD tools, service registries, automation and incident management tools, so that users can visualize the health of the infrastructure through the application up to the business. StackState uses the data it collects to learn about dependencies, allowing it to build a topology of a user's IT environment. Customers will appreciate StackState's openness to integrating with a variety of adjacent tools.

The primary visualization in StackState is the topology map, which highlights problem areas in red. Users can easily view different perspectives, including by application or domain, such as AWS or a particular datacenter. When a problem is occurring, users can examine alerts and view trend graphs. Rather than ingest all data from the many third-party tools, which would incur costs, StackState streams data from the tools – only storing, for instance, the incremental change when a new version of an application is pushed.

If a user wants to examine historical changes in a particular system in an effort to understand root cause, StackState pulls data from the original source to show details of the trend on a graph. We would expect that once StackState points to the likely source of the problem, many users will switch to the third-party tool that originally collected the data, to dig deeper into the trend. This workflow would allow an organization to designate StackState as the central source of truth, eliminating war room debates that ensue when various team members are only able to view a slice of performance data in their specialized tool of choice.

REPORT REPRINT

Users can dig into incidents by moving a slider along a timeline to see when a metric spikes, and correlate that spike with the cause, such as a new code push. The UI element, employed by StackState as well as a number of other vendors, is useful in dynamic environments to enable users to view the order of events as they troubleshoot the root cause.

StackState uses anomaly detection in combination with the topology map it has created of a user's environment in order to intelligently alert users about related problems and their root cause. It is working against a roadmap to first build a causal graph so that early next year it can start predicting incidents for customers, and identifying the root cause, impact of the incident, trigger of the incident, and a timeline.

In April or May, StackState will begin collecting traces via its agent, using the information to offer insight about throughput, latency and errors per second for monitored services. Later, in the third quarter, it plans to make available a distributed tracing offering that will include a waterfall visualization of spans and their durations. Also in the third quarter, StackState is planning to begin integrating with third-party distributed tracing tools, including Amazon X-Ray.

StackState is currently only available as software to be deployed by customers, although it's working on a SaaS delivery model. We think a SaaS offering is crucial for vendors in the monitoring space – for the opportunity to capture customers that prefer SaaS, but also for the ability of the vendor to derive insight like benchmarks and best practices by analyzing data collected across customers.

Competition

StackState is among a small set of vendors advancing the segment of event analytics tools. Traditionally, these tools collected and analyzed events in an effort to deliver a more comprehensive view of incidents than could otherwise be had from siloed tools that specialized in offering visibility into just one layer of a service. Some of these event analytics tools, however, have had shortcomings for several reasons, including relying on the user to determine which events to send to the tool, lacking an understanding of topology, or not being able to analyze metrics or other types of data. All of this may make it more difficult for the tools to surface important incidents and identify their cause.

StackState develops a topology and collects more types of data in addition to events, both via its agent and third-party tools, which should help it address some of these shortcomings. We think its approach is reminiscent of Signifai, the vendor recently scooped up by New Relic. Loom Systems is in a similar category. Potential customers should closely examine the integrations with third-party monitoring tools that each of these vendors supports, since each is relatively limited.

StackState also competes with Moogsoft and BigPanda, two vendors that reinvented event analytics over the systems developed by legacy vendors. While Moogsoft has been historically focused on collecting and analyzing events, it is developing new capabilities around collecting and analyzing metrics, and it is also developing techniques for better understanding customer topologies. These developments should make Moogsoft more competitive with the likes of StackState.

We think a handful of monitoring vendors that are expanding horizontally may become competitive to vendors like StackState in the future. Vendors like CA Technologies (with its Digital Operational Intelligence product), Zenoss, Datadog, Dynatrace, AppDynamics and Splunk collect data either themselves or by ingesting data from third-party tools. These vendors are already analyzing this data, or plan to, for similar outcomes as those offered by StackState. OpsRamp, Centerity and Fixstream also fall into this category.

SWOT Analysis

STRENGTHS

StackState has built a system that can efficiently tap into data collected by third-party tools in order to help DevOps and operations professionals quickly identify the root cause of problems.

WEAKNESSES

StackState doesn't have a SaaS offering yet, which not only limits its addressable market but also prevents it from deriving collective intelligence across its customer base. It's also a young company in a crowded market.

OPPORTUNITIES

We think its openness to examining data from a wide variety of sources should position StackState to attract customers interested in using the product for a range of use cases.

THREATS

StackState's most notable threat comes from established monitoring vendors that are expanding horizontally and increasingly replicating the value that StackState sets out to offer.