REPORT REPRINT

Sumo Logic combines log data with app and infrastructure metrics for unified analytics

NANCY GOHRING

21 APR 2016

The company is hoping to grow by applying its analytics technologies to new types of data. In this case, it's adding metrics and letting users view them in tandem with log data.

451 Research®

Sumo Logic has developed a new service that combines its log data with application and infrastructure metrics in a bid to help developers better troubleshoot problems and also appeal to line-of-business users looking for insight into customer behavior or other trends. The service is available now as part of what Sumo is calling an early access program, and the company hopes to further refine the offering for a general-availability release in a few months. The new service advances Sumo's efforts toward helping its customers derive more value from machine data, and is part of the company's strategy to apply its technology to new types of data.

THE 451 TAKE

Sumo is heading in the right direction with its new capability to help users juggle fewer monitoring and management tools. While the service won't offer the holy grail of a single console, it may let some users eliminate one monitoring service. Sumo isn't alone in its attempt to help customers reduce the number of monitoring tools they use. Other big-name vendors are pairing up or similarly adding services that combine log data with application and infrastructure metrics. Still, Sumo is claiming to be the first to natively ingest, index, and analyze structured metrics data and unstructured log data in real time. It should clearly articulate what the new service can do that its competitors can't in order to show users why they should be interested.

CONTEXT

Founded in 2010, Sumo Logic uses machine learning to offer real-time log data analytics. The company has grown quickly recently, now boasting 1,000 customers (compared with 700 in October 2015), and has tripled its employee count from 100 in April 2014 to 300 currently. It says it now supports more than 15 million queries per day, analyzing 100PB a day for users.

Sumo counts enterprises and SMBs among its customers, with the midmarket making up the largest number of customers and enterprises and bringing in the most revenue. Sumo also has 10,000 users of its free service. In 2015 Sumo Logic raised $80m in a funding round led by DFJ Growth, with Institutional Venture Partners, Greylock Partners, Sequoia Capital, Sutter Hill Ventures and Accel Partners also participating. It has raised $160m since inception.

TECHNOLOGY

Sumo collects machine data from applications, infrastructure, the cloud and some Internet of Things endpoints, and lets customers monitor and receive alerts about events. The service uses machine learning for anomaly detection and lets users search and correlate events.

In order to grow, Sumo has been collecting data about new kinds of components and services. For instance, building on the DevOps movement and trends toward microservices and containers, in 2015 Sumo started supporting Docker so that users could collect data about Docker containers, as well as applications running inside the containers. It has also begun offering new Amazon Web Services integrations, bringing insight into AWS VPC Flow Logs, AWS Kinesis and AWS Config.

As part of its latest announcement, Sumo Logic is combining its unstructured log data with structured metrics data. Users will be able to view log and metric data side by side or overlaid with each other.

Sumo believes that the new capability will let users turn to Sumo Logic as a single tool for discovering and troubleshooting problems. Otherwise, users typically have to switch between a monitoring app, where they might discover an issue, and a log management app, where they can drill down to find the source of the problem.

The new service can ingest time-series-based data from Graphite and AWS CloudWatch. Graphite is an open source monitoring tool that stores time series data and offers graphs of the data. It has become the data store of choice among those opting for composable monitoring, where a monitoring architecture is built by piecing together tools, often that are open source, in order to best fit an infrastructure. Sumo uses Graphite because it's an open protocol that developers use to send data collected via a variety of mechanisms, such as CollectD, an open source tool for collecting app data.

With a handful of other vendors – including big names – also offering similar combined log and metrics data services, Sumo should clearly articulate what sets its offering apart from the rest. It is emphasizing that it reworked its back-end in order to handle both structured and unstructured data natively so that it can present combined dashboards. It should take that message one step further to show users what advantage that might bring them compared with similar services from competitors. Sumo has about 10 customers currently using the new service, and plans to continue to tweak the offering over the next 90 days or so, after which it hopes to roll it out to anyone.

STRATEGY

Like other log analytics companies, Sumo is hoping to grow by applying its analytics and machine-learning technologies to additional data, in this case infrastructure metrics. The strategy is a good one, and is already proving to be a way for Sumo to expand beyond its core user base of developer and operations staff to business users, an expansion that many vendors in the market are attempting.

For instance, a large credit card company is using Sumo's new service for threat detection by looking for anomalies in transactions. Another early user is a retailer that is comparing current user behaviors and transactions to the past so that it can determine if behaviors might be cyclical.

Similarly, Sumo's strategy of extending beyond servers to collect machine data from devices closer to the edge appears to be helping it open doors in the line of business. In fact, it said that 10-20% of its growth is coming from the IoT sector. It currently counts a carmaker, television set manufacturer and fast-food chain among its IoT customers.

Still, Sumo says that developer and operations use cases are the company's bread and butter, and that it will continue to court those segments. That's a smart move – while business users could become an important source of revenue for Sumo, for now operations teams typically are the source of budget for log management products.

Sumo joins other log and metrics providers that have similarly tried to show line-of-business users that log data can be useful to them. Most of them say that adoption by business users is relatively rare. We believe that Sumo and others will continue to be used primarily by developers and operations staff with slow take-up from business users.

COMPETITION

With its new offering, Sumo says its customers report that they are hoping to get rid of tools like DataDog and Stackdriver, in favor of a single combined log and metrics service from Sumo Logic. The company also believes that it competes with Graphite and other open source options.

Sumo will indeed compete with StackDriver, which also tracks both log data and operations metrics, albeit not combined within single visualizations. StackDriver users can, however, notice an event on a monitoring graph and then dig into log data to search for the source of the problem.

But Sumo has more formidable competition, most notably in Splunk, which also combines unstructured machine data with structured business data via its IT Service Intelligence product, introduced in September 2015. Prior to launching that product, Splunk was already offering an integration with DataDog that correlates Splunk's log data with metrics that DataDog collects, offering users a lot of the same functionality that Sumo has developed.

Other competitors include Logentries, with its New Relic integration that connects application metrics with log data, and Stackify, which offers both log management and application monitoring, including some integrated capabilities. More broadly, Sumo competes with Splunk, the biggest name in log management. It also faces Loggly and Graylog among log management competitors.

SWOT ANALYSIS

STRENGTHS
Sumo's early successes branching out into business analytics, particularly in the IoT market, may give it a leg up over competitors, many of which are similarly trying to target business users but don't have many real customers to brag about.

WEAKNESSES
Sumo is following Splunk and others to the market with its new metrics analytics service, but hasn't made a strong case for why customers should choose its service over the more established competition.

OPPORTUNITIES
Sumo's real-time data collection and analytics technology, as well as its emphasis on the IoT market, may appeal to line-of-business users, allowing Sumo to expand its customer base.

THREATS
Sumo, like essentially all log management companies, has to contend with Splunk, the dominant market leader. To get ahead, Sumo will need to either beat competitors to market with new offerings or deliver features that competitors will have a hard time replicating.