REPORT REPRINT

Sumo Logic brings Continuous Intelligence to Amazon Web Services

JASON STAMPER

8 OCT 2015

The cloud-native log and data analytics firm has tightened its integration with AWS for what it calls Continuous Intelligence. The company also recently appointed a new CEO from VMware's Cloud Management business unit, and doubled its total funding after an $80m round.

451 Research

Sumo Logic has tightened its integration with AWS for what it calls Continuous Intelligence. The cloud-native log and data analytics firm has also appointed a new CEO, from VMware's Cloud Management business unit, in the last six months and has doubled its funding total so far with an $80m financing round.

THE 451 TAKE

Sumo Logic sounded bullish in our recent briefing with the firm and rightly so: it has surpassed 700 paying customers and says it is adding 120 to 150 new paying customers each quarter. Moreover it brought on a new CEO in November last year, and raised an additional $80m in funding in May this year, taking total funding to just north of $160m. It's unquestionably a very competitive market for log and machine data analytics firms – and there are far larger competitors – but we can't help but be impressed by Sumo Logic's momentum in the cloud.

CONTEXT

Cloud-based machine data analytics platform vendor Sumo Logic was founded in 2010, and is the top software-as-a-service (SaaS) challenger to rival log and machine data analytics vendor Splunk. Ramin Sayar, who previously ran VMware's Cloud Management business unit since early 2010, became Sumo Logic's new president and CEO in November 2014, replacing Vance Loiselle. Loiselle reportedly left Redwood City, California-based Sumo Logic to be closer to family on the East Coast.

Loiselle, a cofounder of BladeLogic and former BMC executive following its acquisition of BladeLogic, had been running Sumo Logic since May 2012. Under Loiselle's guidance, Sumo Logic grew from a tiny startup with only a handful of customers to one that by the time of his departure could boast more than 460 paying customers.

Sumo Logic says the number of paying customers rose to over 700, and that it is adding between 120 and 150 new customers per quarter. In May of this year, Sumo Logic raised another $80m, taking total funding to $160.5m since its 2010 founding. The latest round was led by DFJ Growth. New investor Institutional Venture Partners and existing backers Greylock Partners, Sequoia Capital, Sutter Hill Ventures and Accel Partners also participated in the round.

TECHNOLOGY

In June, Sumo Logic announced the Sumo Logic Collector and Application for Docker now enables DevOps teams to collect any data from the Docker infrastructure, and the applications running within the container, to identify and resolve critical issues. As containers like Docker become more pervasive, monitoring complex service interactions and identifying issues within each component of an application have become more challenging, the company said. The technology offers real-time monitoring of Docker infrastructure including stats, events and container logs.

Then, in August, Sumo Logic announced new integration with Amazon Web Services VPC Flow Logs. AWS' VPC (Virtual Private Cloud) Flow Logs enables customers to capture information about the IP traffic going to and from network interfaces in their private cloud. Flow logs are said to help with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance or use flow logs as a security tool to monitor the traffic reaching an instance.

The Sumo Logic integration with AWS VPC Flow Logs provided organizations with the ability to strengthen their operations, security and compliance, according to the firm. It provides deeper visibility and visualizations into network flows such as source and destination IP addresses, actions taken (Accept/Reject), what VPC subnet or elastic network interfaces were involved, packet and byte count information, the time interval during which the flow was observed, and trending analysis for behaviors over time.

With the latest announcement, the tighter integration with AWS is part of a broader initiative it calls Continuous Intelligence, the company said. It's aimed at offering real-time, machine data analytics. Features include the elasticity customers would expect from a SaaS model (the ability to scale up and down to meet peaks and troughs in demand). It also offers native integration with AWS that enables real-time operational insight from AWS applications and connectors such as AWS CloudTrail, AWS CloudFront, AWS Elastic Load Balancer and Amazon Simple Storage Service (Amazon S3).

Sumo Logic said that it can offer analytics across the full stack, including data in the cloud as well as being able to combine that with data from on-premises infrastructure. There's also machine learning built in that helps companies discover patterns, anomalies and outliers from infrastructure views. The firm emphasized that all of its usual security credentials still apply in the realm of Continuous Intelligence.

As part of the announcement, the firm made the Sumo Logic App for AWS VPC generally available, and also launched a new

app for AWS Config. This provides visualizations and insight for resource inventory, configuration history and configuration change notification.

Finally, the company announced integration with Amazon Kinesis and Amazon CloudWatch Logs. Kinesis is AWS' data streaming offering; the new integration means Kinesis data streams can be ingested directly by the Sumo Logic platform. This real-time ingestion enables customers to process and visualize real-time data from services such as Amazon Cloud-Watch Logs.

CUSTOMERS

As mentioned Sumo Logic claims to have just over 700 paying customers, up from 460 in November of last year. It says it has around 10,000 active users of Sumo Logic Free, the free version restricted to ingesting 500MB per day (the Professional version starts at $90 per month for up to 1GB per day; there's an Enterprise version with customized plans). It clearly hopes to convert as many of the free customers into Professional or Enterprise customers as their needs grow. Among its 700 paying customers are the likes of Airbnb, Alaska Airlines, Marriott, Australia Post, Citibank, Betfair and the BBC.

Of the latest enhancements, Sumo Logic customer Interactive Intelligence said it uses Sumo Logic's App for Amazon VPC Flow Logs to capture and analyze traffic flow for all of its network interfaces and it also uses the Amazon Kinesis Connector, which enables the firm to send its data stream directly to Sumo Logic for real-time analysis.

Further out this year, the company is considering offering some sort of integration into the NoSQL database MongoDB, although details are thin.

COMPETITION

The 600-pound gorilla in the log and data analytics space is Splunk, which says it surpassed the 10,000 customer mark. Splunk launched its own cloud version in the Americas in 2013, and extended this internationally in April of this year, but the vast majority of Splunk's customers opt for the on-premises rather than the cloud version (it will only say that it has 'hundreds' of customers for its cloud version). Additionally, Splunk Cloud is only available on AWS. Sumo Logic, on the other hand, is available on a number of clouds including AWS, Microsoft Azure, IBM SoftLayer and Heroku, the cloud platform acquired by Salesforce.com in 2010.

Other log management firms – all of which have expanded beyond log analytics into the analysis of other types of machine data – include Tibco (which acquired LogLogic); LogRhythm; Loggly and Logentries. Startup X15 Software offers a cloud-based log management offering based on the open source data processing platform Hadoop, something it has in common with DataTorrent.

Prospects might also consider Cloudera Impala, the open source project for real-time queries on Hadoop. This is less tailored to the analysis of log and machine data, however. For even more basic needs, AWS offers its own Amazon CloudWatch logs that can be used to monitor, store and access log files from Amazon EC2 instances, AWS CloudTrail and other sources.

SWOT ANALYSIS

STRENGTHS
A cloud-based log and machine data analytics platform that runs on numerous cloud platforms, although the tightest integration continues to be with AWS. The recent funding round should give prospects confidence.

WEAKNESSES
Sumo Logic at times struggles to make its case against the largest rival in the space, Splunk, despite the fact we think it can go toe to toe with the Splunk Cloud offering.

OPPORTUNITIES
Sumo Logic notes there are 10,000 users of its free version, which it hopes to convert to Professional or Enterprise customers as their data ingestion needs and support requirements grow.

THREATS
It's a very competitive space, and for the very lowest latency requirements, some companies will continue to opt to analyze their logs as close to source as possible. In some cases, that means on-premises rather than in the cloud