REPORT REPRINT

Sumo Logic rolls out new siem, promises more advanced analytics

NANCY GOHRING, ERIC OGREN

20 SEP 2018

The company recently announced a new SaaS SIEM product. The idea is to deliver a cloud SIEM offering that collects logs from apps and security products, and then analyzes and correlates the data in order to identify security issues.

451 Research®

Sumo Logic recently announced a new SaaS SIEM product. The idea is to deliver a cloud SIEM offering that collects logs from apps and security products, and then analyzes and correlates the data in order to identify security issues. In addition to the SIEM, Sumo Logic is talking up its work around mining data across its user base in order to surface recommendations for individual customers. Vendors with cloud-delivered offerings like Sumo's are in a good position to develop these types of valuable capabilities, which are based on applying advanced analytics technologies like machine learning to data collected from their customers, although we're only just beginning to see actual features built on that concept emerge in the market.

THE 451 TAKE

Sumo Logic continues to add customers and expand within those it has, reporting good growth in terms of new users and average revenue. Sumo's dedication to machine learning technologies has led to it supporting organizations that are on the cutting edge of machine learning adoption, particularly those that view IT ops data as an important potential source of intelligence when analyzed alongside other business data. Sumo's expansion into the security realm is a natural – it makes sense to serve both IT ops and security use cases. However, the security sector is very crowded, and Sumo faces the same hurdle as some of its peers in terms of organizational challenges that make it hard for security and IT ops teams at its customers to share tools.

CONTEXT

Founded in 2010 and based in Redwood City, California, Sumo Logic has raised $235m in funding, including a $75m round of financing in 2017. Investors include Sapphire Ventures, Accel Partners, DFJ, Greylock Partners, Sequoia Capital, Institutional Venture Partners and Sutter Hill Ventures.

Sumo Logic acquired FactorChain in January for its integrated incident-response workflow technology. Dave Frampton, formerly CEO of FactorChain, is now spearheading Sumo's re-entry into security operations markets.

Sumo reports that it added 170 new customers in Q2, bringing its customer count up to 1,600. Users include Pokemon, Marriott, Salesforce, Virgin Money and Informatica. Customers often start out small, according to Sumo, but quickly expand their usage. In the second quarter, Sumo graduated from two-digit average recurring revenue to three-digit ARR.

The company now has 400 employees, with expansion happening essentially across the board. It has made sales hires in Japan and Germany (and added an availability zone in Frankfurt), which may drive additional hiring and sales in those regions.

PRODUCTS

Sumo is primarily thought of as a log analytics vendor, serving both IT operations and security use cases, although it added support for collecting metrics in 2016 – very early in the currently popular trend of collecting and correlating both metrics and logs. It promotes its ability to return results quickly.

At its Illuminate customer conference in mid-September, Sumo announced a new SaaS SIEM product. The idea is to deliver a cloud SIEM offering that collects logs from apps, as well as a host of security products, including Carbon Black endpoints, Palo Alto virtual firewalls, zScaler, AWS GuardDuty, Okta and OneLogin, and then analyzes and correlates the data in order to identify security issues. Sumo plans to build on the investigation workflow technology it recently acquired from FactorChain to enable customers to not only identify suspicious activity, but also manage incident response.

Sumo envisions accelerated DevOps cycles shifting the balance of requirements for modern security operations from traditional security log data toward IT operations data. For instance, a container may launch, execute and expire before log data is ever recorded by an SIEM, but IT operations data will be able to give SecOps and analytics engines the timely visibility necessary to provide security oversight. Sumo Logic has successfully architected operations data analytics for cloud environments, and plans to use those strengths for a differentiated SIEM offering. The Sumo Logic SIEM will integrate IT operations and security data with an eye on modern DevOps deployment cycles.

Sumo was already catering to the security use case, but we think the FactorChain acquisition and the creation of a dedicated team focused on developing security offerings indicate that it hopes to ensure its offering is competitive with security- and log-centric products. The challenge it faces is that its vision is best realized by organizations that use Sumo for both IT operations and security. We've found that those teams often prefer to make their own individual buying decisions, which may mean that both teams don't want to adopt Sumo. Sumo and others are beginning to demonstrate the value of sharing tools, which may help to break down this hurdle in time.

Sumo also continues to invest in technology that analyzes anonymized data across customers in order to present individual customers with recommendations and other insight specific to their IT environments. It is still in the early stages of developing these offerings, with Community Insights an initial offering in this category. With Community Insights, users will be able to view benchmarks of their peers about things like performance and choosing the right cloud service for particular workloads.

Sumo has a few data scientists dedicated to further developing these capabilities, notably in ways that won't require customers to consult a dashboard to discover industry benchmarks, but instead proactively surface insight to customers. Sumo envisions some particularly interesting security features that might, for instance, alert users that are experiencing a security event in a different way than their peers.

We see just a few vendors in the application and infrastructure performance market attempting to harness the experiences of all users to guide individual users, and we think doing so has the potential to add significant value for end users. Logz.io is a leader here, with an offering that mines data across its customer base, as well as online sources, in order to pull in relevant data for customers. Zenoss is also developing these capabilities. We like Sumo's vision here, but note that the vendor has been working on this for a while, with only an initial deliverable available – we heard from Sumo about similar plans in late 2016.

Sumo has also made some integrations targeted at businesses that want to feed data collected by Sumo into machine learning engines. One such integration is with Jupyter, the number one machine learning tool in use, according to our recent 451 Research, Voice of the Enterprise: Artificial Intelligence/Machine Learning 2018 report. Sumo also now has an integration with Google Cloud's TensorFlow libraries so that users can run custom machine learning algorithms on their data in Sumo.

Other product enhancements include a reworked API framework based on Swagger, a refreshed role-based access control system and a Search Templates feature that is designed to make it easier for people to use Sumo without learning the Sumo query language. Sumo is also offering a logs-to-metrics capability designed to extract KPIs from logs, and has upped its support for microservices environments and Kubernetes. All of these updates indicate that Sumo is keeping a close eye on new technology adoption patterns and responding to them.

COMPETITION

For virtually all log analytics vendors, Splunk is the one to beat. Sumo may win out over Splunk at businesses that value the benefits inherent to a cloud-native service like Sumo, including ease of signup and scaling. Generally speaking, Splunk offers probably the widest set of features and capabilities of any log vendor out there. But many customers and potential customers we talk to say that if they don't use many of those capabilities, Splunk might not be worth the price tag.

Sumo may compete with Devo (the recently renamed Logtrust) and Loggly, which has been acquired by SolarWinds, although SolarWinds tends to appeal to SMBs, and Sumo has enterprise aspirations.

In IT ops, in particular, Sumo may find itself competing with vendors that started out collecting metrics for monitoring use cases but have expanded to deliver integrated log analytics. This is a popular topic currently, with Datadog buying Logmatic to enable this type of integration, and other vendors (including Dynatrace and Zenoss) investing in further developing their log analytics capabilities. Others, including Elastic and Sematext, do integrated logs and metrics as well, and Splunk recently built a new back end to collect and analyze metrics.

Among SIEM providers, Sumo will find itself up against AlienVault USM AnyWhere, IBM QRadar with Resilient, LogRythym CloudAI, McAfee Enterprise Security Manager with Investigator, MicroFocus ArcSight with Investigate, Rapid7 with Insight and Splunk with Caspida in deals for adding cloud applications to SOC responsibilities.

SWOT ANALYSIS

STRENGTHS

Sumo was very early among vendors to combine logs and metrics in a way that serves an IT ops monitoring and troubleshooting use case, and has the potential to expand into new business-centric use cases.

WEAKNESSES

As a relatively new vendor in the crowded security sector, Sumo has its work cut out for it making a name for itself.

OPPORTUNITIES

Sumo has kept up with technology adoption trends among its customer base in order to quickly respond to the requirements of users of those technologies. As such, it is well positioned to meet the needs of the growing base of businesses using tools like Kubernetes and microservices architectures.

THREATS

New log analytics vendors crop up with regularity – most plainly targeting Splunk – putting Sumo (and other more established log vendors) in the position of constantly defending against new entrants harnessing the latest technologies.